"EXIT charts" em códigos turbo e LDPC – o que são e para que servem?

© Sílvio A. Abrantes
Departamento de Engenharia Electrotécnica e de Computadores
Faculdade de Engenharia, Universidade do Porto
Porto, Portugal
sam@fe.up.pt

Abril de 2006

Resumo: Neste texto é feita a apresentação detalhada dos "EXIT charts", um dos mais importantes métodos de avaliação do desempenho da descodificação iterativa de códigos e sistemas turbo e de códigos LDPC. A exposição é acompanhada por diversos exemplos de cálculo com os dois tipos de códigos citados.

Palavras-chave: códigos turbo, códigos LDPC, processamento turbo, descodificação iterativa, informação mútua média, "EXIT Charts".

1. Introdução

Neste artigo faz-se a apresentação dos "EXIT charts"[1], gráficos que quantificam a transferência de informação extrínseca entre descodificadores na descodificação iterativa. Inventados pelo alemão Stephan ten Brink em 1999 [1], desde então têm-se revelado muito úteis na avaliação do desempenho e na ajuda ao projecto de códigos e sistemas turbo e códigos LDPC[2]. A original ideia de ten Brink foi a de utilizar um dos conceitos-chave da Teoria da Informação, de Claude Shannon – a informação mútua média – para monitorizar a descodificação iterativa de códigos turbo, apresentados ao público meia dúzia de anos antes, em 1993 [2]. Da codificação turbo depressa os "EXIT charts" foram aplicados aos códigos LDPC e com igual sucesso.

O artigo está estruturado da seguinte forma: na Secção 2 é feita uma breve revisão da descodificação iterativa baseada em razões de verosimilhança LLR; a Secção 3 aborda a avaliação do desempenho da descodificação iterativa através da evolução da informação mútua média e indica como se calculam as funções de transferência, ou funções EXIT, dos blocos descodificadores turbo; na Secção 4 mostra-se como se obtêm os "EXIT charts" correspondentes às funções EXIT da Secção 3; a Secção 5, a última, trata dos "EXIT charts" de códigos LDPC regulares e irregulares em canais gaussianos e em canais binários com rasuras (canais BEC[3]), fazendo-se aí menção às interessantes propriedades da dualidade e da área. O texto termina com a inclusão de vários Apêndices: os dois primeiros apresentam algumas propriedades de funções densidade de probabilidade simétricas e consistentes e certas relações entre LLR condicionais; o Apêndice A3 concentra num só local diversas expressões da informação mútua média, o Apêndice A4 apresenta a dedução analítica dos limiares de convergência dos códigos LDPC regulares e o Apêndice A5 mostra como as percentagens de ramos e de nós de códigos LDPC irregulares estão relacionadas entre si.

2. Descodificação iterativa ou turbo

Considere-se a Fig. 1. O bloco "Codificador" designa quer um codificador turbo ou LDPC quer um sistema turbo genérico[4], o bloco "Descodificador" é um descodificador MAP ("maximum a posteriori probability"), X e $\hat{X}$ representam sequências de bits ± 1 e Y representa uma sequência de símbolos (por exemplo valores reais). Com codificação turbo o descodificador MAP está equipado com um dos algoritmos BCJR, log-MAP, max-log-MAP ou SOVA [3] e com codificação LDPC usa o algoritmo da *soma-e-produto* para

[1] EXIT = "Extrinsic Information Tranfer".
[2] LDPC = "Low-Density Parity-Check".
[3] BEC = "Binary Erasure Channel".
[4] Um sistema turbo genérico é um sistema concatenado que pode representar, entre outros exemplos, igualização turbo, modulação turbo, codificação conjunta de fonte e de canal e recuperação iterativa da temporização. Em qualquer caso existe sempre um codificador no emissor e a descodificação/desmodulação é feita iterativamente.

transferência de mensagens (“message-passing”, em inglês) [4]. O bloco “Canal” representa um canal de comunicações genérico: pode ser um canal binário simétrico, um canal binário com rasuras, um canal de ruído branco gaussiano aditivo[5] ou outro qualquer.

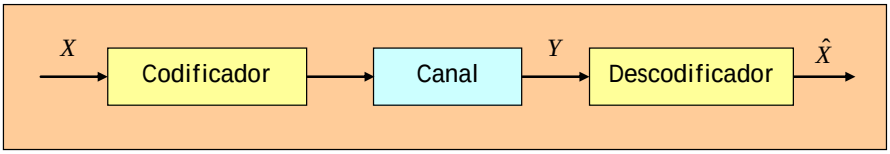

Fig. 1. Um sistema de codificação/descodificação genérico.

Tratando-se de um codificador ou de um sistema turbo a codificação é feita de modo concatenado em série ou em paralelo, como se mostra nas Figs. 2 e 3. Os blocos descodificadores[6] MAP1 e MAP2 presentes no receptor das figuras são blocos “soft-in soft-out”, ou SISO, ou seja, aceitam e produzem informações brandas as quais, normalmente, são números reais que resultam de expressões logarítmicas abreviadamente referidas como LLR (de “Log-Likelihood Ratio”). É o que iremos considerar para as entradas e saídas L_1, L_2, L_{a1}, etc., dos descodificadores. As LLRs mencionadas são assim definidas:

$L_a(x) = \ln \frac{p(x=1)}{p(x=-1)}$	*LLR a priori*
$L(\mathbf{y} \mid x) = \ln \frac{p(\mathbf{y} \mid x=1)}{p(\mathbf{y} \mid x=-1)}$	*LLR condicional a priori* (“do canal”)
$L(x \mid \mathbf{y}) = \ln \frac{p(x=1 \mid \mathbf{y})}{p(x=-1 \mid \mathbf{y})}$	*LLR condicional a posteriori*
$L_e(x) = L(x \mid \mathbf{y}) - L_a(x) - L(\mathbf{y} \mid x)$	*LLR extrínseca*

Nas expressões anteriores $p(x|\mathbf{y})$ e $p(\mathbf{y}|x)$ representam ou probabilidades ou funções densidade de probabilidade (consoante Y seja uma variável aleatória (v.a.) discreta ou contínua).

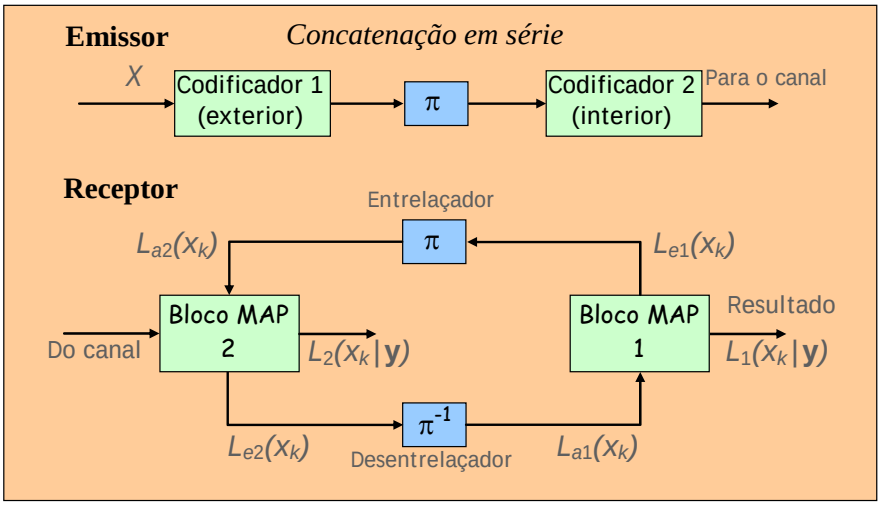

Fig. 2. Emissor e descodificador iterativo para concatenação em série.

[5] A este tipo de ruído vamos chamar, abreviadamente, ruído AWGN, de “Additive White Gaussian Noise”.
[6] Ao longo do texto os termos “bloco” e “descodificador” são usados como sinónimos. Num sistema turbo genérico o termo “descodificador” pode, por isso, representar um bloco desmodulador, por exemplo.

Prova-se no Apêndice A2 que tendo sido recebida uma sequência de valores reais y na presença de ruído AWGN de variância $\sigma^2 = \frac{1}{2\,E_s/N_0} = \frac{1}{2R_c\,E_b/N_0}$ a LLR condicional a priori é igual a

$$L(\mathbf{y} \mid x) = \frac{2}{\sigma^2}\,y = \frac{4E_s}{N_0}\,y = 4R_c\,\frac{E_b}{N_0}\,y\,,$$

em que E_s é a energia do bit transmitido (depois de codificado), E_b é a energia do bit antes da codificação, $R_c = k/n$ é a taxa do código e $N_0/2$ é a densidade espectral de potência do ruído AWGN à saída do filtro adaptado do receptor. Ou seja, $L(\mathbf{y}|x)$ depende da relação sinal-ruído e do valor y recebido do canal.

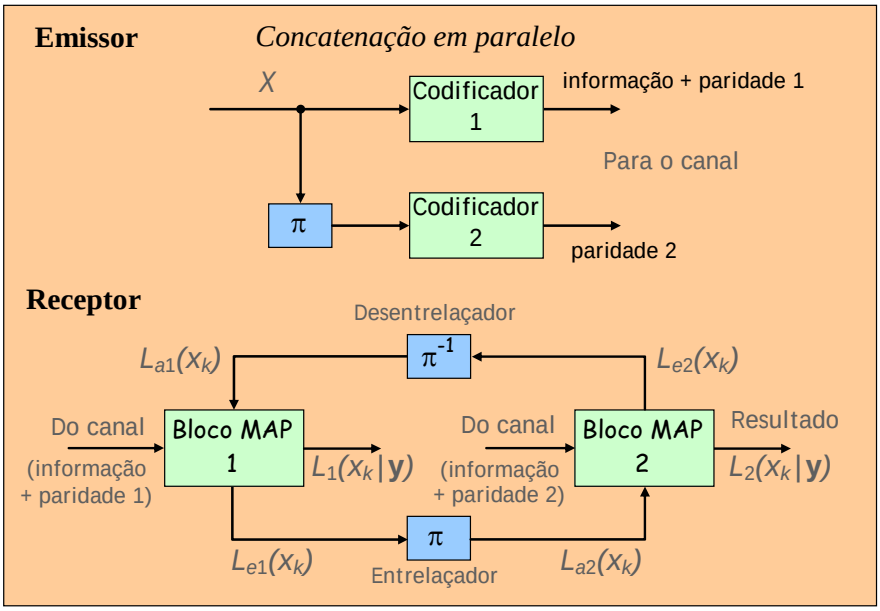

Fig. 3. Emissor e descodificador iterativo para concatenação em paralelo.

Voltemos aos blocos descodificadores das Figs. 2 e 3:

- nas entradas aplica-se a LLR a priori proveniente do descodificador anterior, L_a, e a informação proveniente do canal, $L(\mathbf{y} \mid x) = \frac{4E_s}{N_0}\,y$ (excepto no descodificador exterior (bloco MAP1) da concatenação em série (cf. Fig. 2), que não tem entrada vinda do canal[7]);
- nas saídas recolhem-se a LLR a posteriori $L(x|\mathbf{y})$ e a LLR da informação extrínseca, $L_e(x)$. Esta transforma-se, após entrelaçamento (π) ou desentrelaçamento (π^{-1}), na LLR a priori do descodificador seguinte.

Tomando como exemplo a concatenação em paralelo o processo de descodificação iterativa funciona assim: na primeira metade de cada iteração o descodificador 1 produz a informação extrínseca L_{e1} que, "convertida" na LLR a priori L_{a2}, é aplicada ao descodificador 2; na segunda metade o descodificador 2 produz L_{e2} que, "convertida" na LLR a priori L_{a1}, é aplicada ao descodificador 1. O processo prossegue repetindo-se iteração após iteração. De notar que os entrelaçadores e desentrelaçadores não alteram os valores das sequências que lhes são aplicadas, alteram apenas as respectivas posições relativas. E como se deseja assegurar independência estatística entre os descodificadores são sempre usados entrelaçadores muito grandes.

Note-se bem: o que circula entre blocos, de iteração para iteração, é a informação extrínseca, e só ela.

[7] Ou então consideramos nula a entrada "do canal" se quisermos que o descodificador exterior tenha duas entradas como os outros.

3. Avaliação do desempenho da descodificação iterativa através de "EXIT charts"

3.1 Métodos de avaliação do desempenho da descodificação iterativa

Ao falarmos de descodificação iterativa podemos perguntar: quantas iterações serão necessárias para que, com um dado esquema de codificação, se atinja uma determinada probabilidade de erro? E será possível atingir essa probabilidade de erro, mesmo com um número elevadíssimo de iterações? A probabilidade de erro está a baixar muito ou pouco de iteração para iteração? Ganharemos muito se em vez de, por exemplo, dez iterações, usarmos quinze ou, pelo contrário, não compensa? Vale a pena continuar com as iterações ou os ganhos de codificação já são diminutos? Para responder a estas e outras perguntas precisamos de avaliar a "qualidade" da informação extrínseca que circula entre descodificadores de iteração em iteração e para isso há vários métodos de avaliação possíveis [5]. Todos têm em comum o acompanhamento ou a monitorização ao longo das iterações de um dado parâmetro considerado adequado. Por exemplo, poderia seguir-se a evolução da função densidade de probabilidade (fdp) da informação extrínseca circulante[8] – método designado por "density evolution" e originalmente proposto por Richardson e Urbanke em 2001 para o projecto de códigos LDPC [6] [7]. Ou poderia seguir-se a evolução da média dessa fdp [8]. Ou ainda, poderia monitorizar-se a variância de um erro, como se faz em [9] num ambiente de igualização turbo, ou a variância de ruído em CDMA, como em [10]. A ferramenta que nos interessa é a que se baseia no acompanhamento da evolução da *informação mútua média* entre a informação extrínseca L_e e a sequência binária original X ao longo das iterações. O gráfico que se obtém é o "EXIT chart"[9]. Veremos adiante que, afortunadamente, *não é necessário simular a descodificação iterativa* para construir "EXIT charts".

3.2 Informação mútua média, funções de transferência e "EXIT charts"

Sabe-se da Teoria da Informação que a informação mútua média entre as variáveis X e Y é definida como

$$I(X;Y) = H(X) - H(X \mid Y) = H(Y) - H(Y \mid X)$$

em que $H(X)$ e $H(Y)$ são as entropias de X e Y, respectivamente, e $H(X|Y)$ e $H(Y|X)$ são entropias condicionais. No Apêndice A3 são apresentadas definições equivalentes aplicáveis a variáveis discretas e contínuas.

Para o traçado dos "EXIT charts" vamos precisar das seguintes informações mútuas médias:

- $I_A = I(X;L_a)$, entre a sequência de informação X e a sequência de entrada L_a de cada descodificador;
- $I_E = I(X;L_e)$, entre a mesma sequência de informação X e a sequência de saída L_e de cada descodificador.

S. ten Brink propôs que se observasse a evolução temporal de I_E em função da evolução temporal de I_A. Assim, tal como L_{a1}, L_{a2}, L_{e1} e L_{e2} também I_{A1}, I_{A2}, I_{E1} e I_{E2} vão circular entre descodificadores, desta maneira:

$$I_{A1} \rightarrow I_{E1} = I_{A2} \rightarrow I_{E2} = I_{A1} \rightarrow I_{E1} = I_{A2} \rightarrow I_{E2} = \ldots$$

Começando em $I_{A1} = 0$ no primeiro descodificador, observar-se-á então que ao longo das iterações I_{Ai} e I_{Ei} vão crescendo (até, espera-se, $I_{Ei} = 1$). Os diversos valores de I_A e I_E que vão sendo obtidos estabelecem, portanto, um mapeamento entre a entrada I_A e a saída I_E de cada bloco, ou seja, definem uma *função de transferência* de informação do bloco, hoje em dia também chamada *função EXIT*. Designando-a por T escrevemos

$$I_E = T(I_A, E_s/N_0)$$

[8] Neste caso não é, em rigor, um parâmetro que se monitoriza mas toda uma função. É um método computacionalmente exigente.

[9] Como curiosidade registe-se que originalmente ten Brink chamou "EIT" e não "EXIT" aos seus gráficos. O termo (feliz) "EXIT" só começaria a ser utilizado mais tarde.

ou, se fixarmos E_s/N_0, simplesmente $I_E = T(I_A)$, como se ilustra na Fig. 4. A função EXIT pode até nem depender da razão E_s/N_0. É o que acontece no descodificador exterior (bloco MAP1) da concatenação em série pois esse bloco não tem nenhuma entrada vinda do canal.

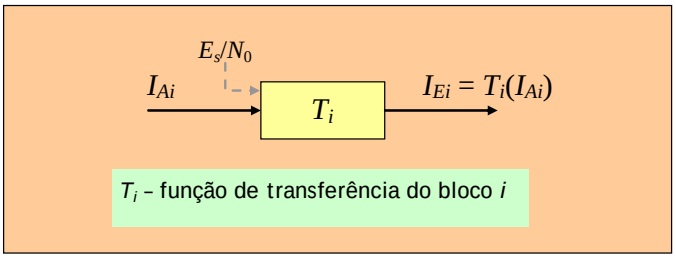

Fig. 4. A função de transferência T_i de um bloco MAP_i, entendida como uma correspondência entre as informações mútuas médias de entrada e de saída.

A Fig. 5 é uma adaptação da Fig. 3 usando informações mútuas médias em vez de LLRs (idêntica adaptação se poderia fazer na Fig. 2). Aí se indica que $I_{A2} = I_{E1}$ e $I_{A1} = I_{E2}$, pois o entrelaçamento e o desentrelaçamento não alteram o valor da informação mútua média.

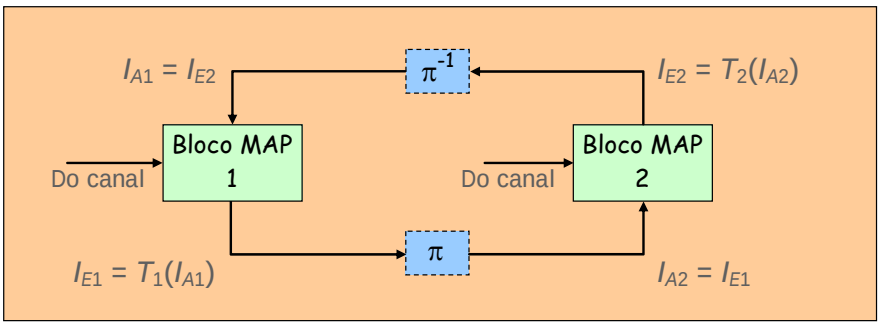

Fig. 5. Utilização da informação mútua média na descodificação iterativa para concatenação em paralelo.

Os valores de I_{A1}, I_{A2}, I_{E1} e I_{E2} variam, como se disse, com a iteração n da descodificação e estão confinados ao intervalo [0;1]. Por exemplo, a informação mútua média I_{E1} produzida na enésima iteração (seja $I_{E_1}^{(n)}$) depende do valor de $I_{A1} = I_{E2}$ produzido pelo bloco 2 na iteração anterior; de igual modo o valor de I_{E2} produzido na segunda metade da enésima iteração, $I_{E_2}^{(n)}$, depende de $I_{A2} = I_{E1}$ produzido na primeira metade da mesma iteração. Ou seja:

$$\begin{aligned} I_{E_1}^{(n)} &= T_1\left[I_{A_1}^{(n-1)}\right] \\ I_{A_2}^{(n)} &= I_{E_1}^{(n)} \\ I_{E_2}^{(n)} &= T_2\left[I_{A_2}^{(n)}\right] \\ I_{A_1}^{(n)} &= I_{E_2}^{(n)} \end{aligned} \qquad (1)$$

Estas relações traduzem-se nas representações gráficas das funções I_{E1} em função de I_{A1} e I_{E2} em função de I_{A2} mostradas na Fig. 6a, onde os pontos n.1 e n.2 indicam a primeira e a segunda parte da iteração n, respectivamente. Esta figura confirma o que poderíamos antecipar mesmo sem conhecermos T_1 e T_2: numa descodificação iterativa bem sucedida as funções EXIT devem ser funções crescentes, isto é, a informação mútua média à saída de cada bloco (I_{E1} ou I_{E2}) deve ser superior à informação mútua média na sua entrada (I_{A1} ou I_{A2}). E porquê? Porque se queremos ter cada vez menos dúvidas acerca de X à medida que as iterações decorrem, então da entrada para a saída de cada bloco deve ocorrer uma redução da incerteza remanescente acerca dos símbolos X, redução traduzida pela informação mútua média, como se sabe da Teoria da Informação. À medida que as iterações decorrem as informações extrínsecas vão, portanto, aproximando-se de 1. A avaliação do desempenho de cada descodificador pode então ser feita à custa da representação gráfica da sua função EXIT. Ora acontece

que no caso de se usarem entrelaçadores e desentrelaçadores de grande comprimento, como é costume, os descodificadores tornam-se independentes entre si, o que tem uma consequência importante: podemos determinar as funções de transferência T_1 e T_2 separadamente para cada descodificador sem termos de proceder à descodificação iterativa ao longo de várias iterações. O que é preciso é, para cada descodificador, colocar na entrada sequências a priori L_a adequadas e observar na saída as correspondentes sequências extrínsecas L_e. Só que cada sequência de valores L_a (e L_e) só dá origem a um valor de I_A (e I_E), o que quer dizer que se quisermos determinar uma função T precisamos de obter vários pares de pontos (I_A, I_E), isto é, temos de previamente obter outros tantos pares de sequências L_a e L_e. Como fazer?

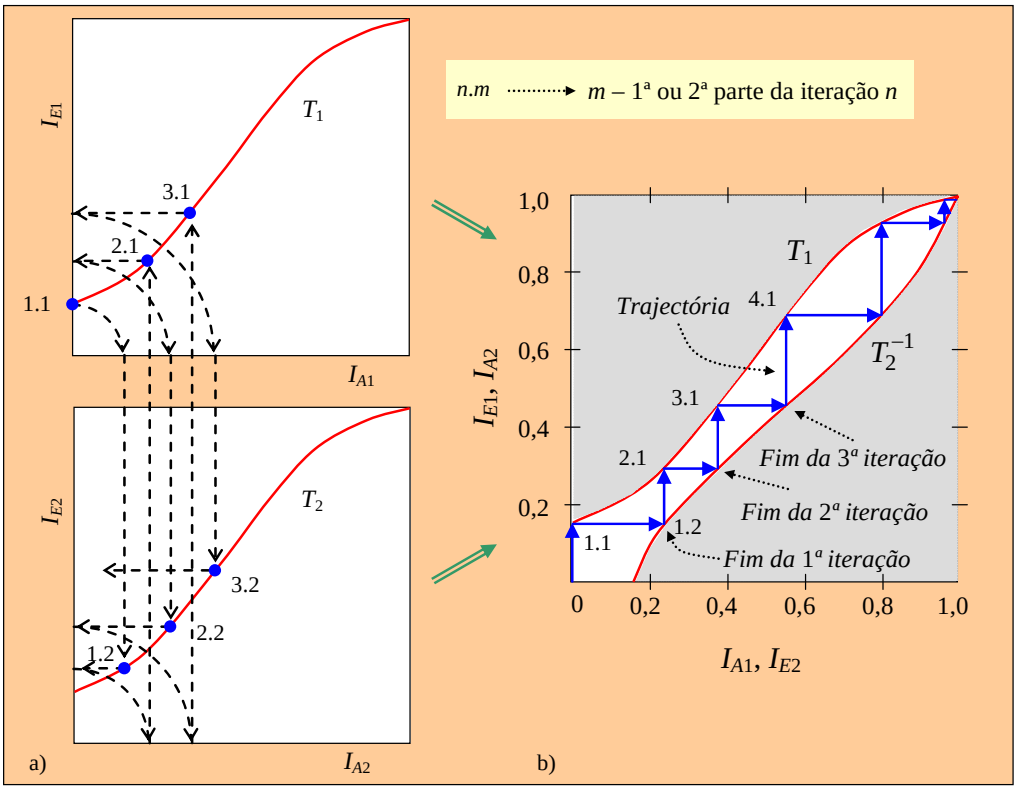

Fig. 6. Como se constrói um "EXIT Chart" (exemplo com codificadores iguais): a) duas funções EXIT iguais; b) o "EXIT chart" correspondente.

Na descodificação turbo a saída de um bloco MAP é a entrada do outro (desprezando π e π^{-1}). Então podemos usar o mesmo sistema de eixos para fazer a representação conjunta (trocando, é claro, os eixos de um dos dois gráficos, como se mostra na Fig. 6b). Com um único sistema de eixos e duas funções EXIT nele representadas surge então um percurso em escada composto de segmentos horizontais e verticais que "salta" alternadamente de uma curva para a outra, começando no gráfico da função T_1 com valor inicial arbitrado $I_{A_1}^{(0)} = 0$, no ponto 1.1, e prosseguindo sucessivamente para os pontos 1.2, 2.1, 2.2, 3.1, etc. Podemos assim visualizar uma *trajectória de descodificação iterativa* entre as duas funções de transferência (que assim parecem ser as paredes de um túnel). É isto o "EXIT chart"!

Na descodificação iterativa atinge-se o canto superior direito do gráfico se e só se houver um túnel de escape como nas Figs. 6, 7 e 12. A Fig. 12a ilustra também a situação contrária, aquela em que o túnel não tem saída ("EXIT") por as funções T_1 e T_2^{-1} se intersectarem na diagonal a tracejado[10].

Os gráficos da Fig. 6 correspondem à utilização de dois codificadores iguais, daí que T_1 seja igual a T_2. A Fig. 7 apresenta outro exemplo de um "EXIT chart" mas agora com codificadores diferentes. Ambas as figuras correspondem a um determinado valor de E_s/N_0. Com valores mais elevados de E_s/N_0 o túnel ficaria mais largo e com valores mais baixos ficaria mais estreito, de modo que no primeiro caso o canto superior direito,

[10] As funções T_1 e T_2^{-1} só estão desenhadas até à sua intersecção na diagonal.

correspondente a $I_E = 1$, seria atingido em menos iterações, e no segundo caso esse canto poderia até nem ser alcançado caso as duas curvas, ou paredes do túnel, se encontrassem prematuramente e deixasse de haver túnel – o que, com codificadores iguais, ocorre necessariamente na diagonal que une o ponto de coordenadas (0,0) ao ponto (1,1). Esta situação de túnel sem saída ocorre quando I_{E2} deixa de crescer de iteração para iteração, isto é, quando $I_{E_2}^{(n+1)} = I_{E_2}^{(n)}$. Como, de acordo com a Eq. (1), $I_{E_2}^{(n+1)} = T_2\left[T_1\left(I_{E_2}^{(n)}\right)\right]$, a condição $I_{E_2}^{(n+1)} = I_{E_2}^{(n)}$ equivale a

$$T_1\left(I_{E_2}^{(n)}\right) = T_2^{-1}\left(I_{E_2}^{(n)}\right) \qquad \text{(ponto de intersecção das curvas)}$$

e indica que o algoritmo de descodificação não converge para uma solução de probabilidade de erro arbitrariamente nula por mais iterações que se considerem. O cruzamento da diagonal está assinalado na Fig. 11 e a ausência de túnel de saída confirmada na Fig. 12a.

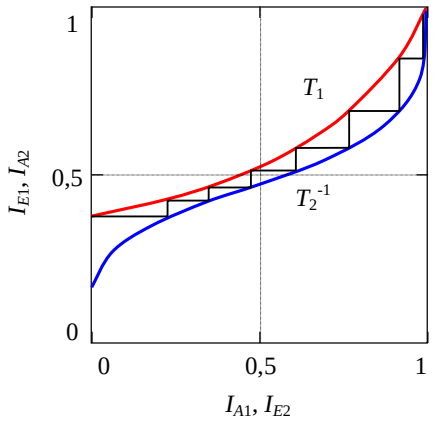

Fig. 7. Outro exemplo de trajectória em "EXIT chart" (com codificadores diferentes).

Já sabemos o que são e como se constroem os "EXIT charts" mas ainda não sabemos como obter as respectivas funções EXIT dos descodificadores. Vamos ver como o fazer, começando primeiro com códigos turbo e prosseguindo depois com códigos LDPC.

4. "EXIT Charts" de turbo-códigos

O Apêndice A3 mostra na Eq. (26) que, independentemente das características estatísticas da LLR extrínseca L_e, a informação mútua média I_E é igual a

$$I_E = I(X;L_e) = \frac{1}{2}\sum_{x\in\{\pm 1\}}\int_{-\infty}^{\infty} p(L_e|x)\log_2\frac{2\,p(L_e|x)}{p(L_e|-1)+p(L_e|1)}dL_e \qquad (2)$$

se os símbolos binários $X = \pm 1$ forem equiprováveis (idêntica expressão é válida para I_A substituindo L_e por L_a). Sabe-se [1] [11] que à medida que as iterações da descodificação decorrem L_e se comporta cada vez mais como uma v.a. gaussiana (e, portanto, a LLR a priori L_a do descodificador seguinte também). Essa aproximação à distribuição normal é muito satisfatória se se considerar que a v.a. é consistente [12], o que implica que o valor médio da v.a. gaussiana é metade da variância (ver Apêndice A1). Nesse caso a informação mútua média I_A vale, segundo a Eq. (27) do Apêndice A3,

$$I_A = I(X;L_a) = 1 - \int_{-\infty}^{\infty} p(L_a|1)\log_2\left(1+e^{-L_a}\right)dL_a\,, \qquad (3)$$

sendo $L_a \sim \mathcal{N}(\pm\sigma_a^2/2, \sigma_a^2)$ e

$$p(L_a\,|1) = \frac{1}{\sqrt{2\pi\sigma_a^2}} \exp\left[-\frac{(L_a - \sigma_a^2/2)^2}{2\sigma_a^2} \right].$$

I_A é calculada por integração numérica. Como se vê, $p(L_a|1)$ e, portanto, I_A dependem apenas de um parâmetro (a variância σ_a^2 ou o valor médio $\sigma_a^2/2$ de L_a), o que é uma vantagem, permitindo que, se necessário, pares de valores (σ_a, I_A) sejam guardados em tabela para uso posterior. Podemos, assim, definir a função real de variável real não negativa

$$I_A = J(\sigma_a)\,,\ \ \sigma_a \geq 0 \tag{4}$$

de contradomínio [0;1], representada graficamente na Fig. 8. Como $I_A(\sigma_a = 7,2) \approx 1$, não é necessário considerar valores de σ_a superiores a cerca de 7,2.

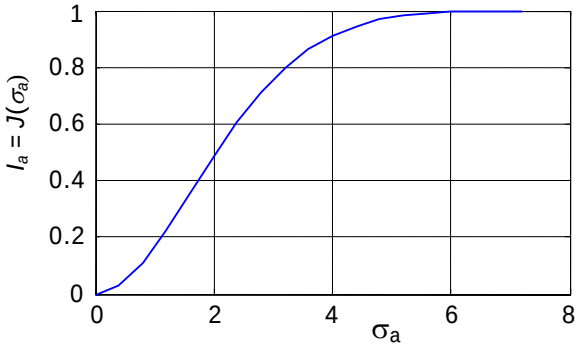

Fig. 8. A informação mútua média I_A em função do parâmetro único σ_a.

Aparte: a informação mútua média I_A dada pela Eq. (3) pode ser obtida sem integração se usarmos a excelente e facilmente utilizável aproximação polinomial e exponencial proposta por ten Brink *et al.* [16]:

$$I_A = J(\sigma_a) \approx \begin{cases} a_{j1}\sigma_a^3 + b_{j1}\sigma_a^2 + c_{j1}\sigma_a & 0 \leq \sigma_a \leq \sigma^* \\ 1 - e^{a_{j2}\sigma_a^3 + b_{j2}\sigma_a^2 + c_{j2}\sigma_a + d_{j2}} & \sigma^* < \sigma_a < 10 \\ 1 & \sigma_a \geq 10 \end{cases} \tag{5}$$

em que $\sigma^* = 1,6363$ e

$$a_{j1} = -0,0421061 \quad b_{j1} = 0,209252 \quad c_{j1} = -0,00640081$$
$$a_{j2} = 0,00181491 \quad b_{j2} = -0,142675 \quad c_{j2} = -0,0822054 \quad d_{j2} = 0,0549608$$

Os mesmos autores usam uma aproximação do mesmo género para calcular a função inversa $J^{-1}(\,)$:

$$J^{-1}(I) \approx \begin{cases} a_{\sigma 1} I^2 + b_{\sigma 1} I + c_{\sigma 1}\sqrt{I} & 0 \leq I \leq I^* \\ -a_{\sigma 2}\ln\left[b_{\sigma 2}(1-I)\right] - c_{\sigma 2} I & I^* < I < 1 \end{cases} \tag{6}$$

com $I^* = 0,3646$ e

$$a_{\sigma 1} = 1,09542 \quad b_{\sigma 1} = 0,214217 \quad c_{\sigma 1} = 2,33727$$
$$a_{\sigma 2} = 0,706692 \quad b_{\sigma 2} = 0,386013 \quad c_{\sigma 2} = -1,75017$$

O integral da Eq. (3) representa o valor esperado de $\log_2\left(1+e^{-L_a}\right)$ pelo que normalmente [12] também podemos escrever

$$I_A = I(X;L_a) = 1 - E\left[\log_2\left(1+e^{-L_a}\right)\right] = E\left[\log_2 \frac{2}{1+e^{-L_a}}\right]. \tag{7}$$

O cálculo do valor esperado requer o conhecimento de conjuntos grandes de valores de X e de L_a. Assim, se tivermos N valores binários (±1) x_1, x_2, …, x_N de X e N amostras gaussianas e consistentes L_{a1}, L_{a2},…, L_{aN} de L_a a informação mútua média I_A da Eq. (7) pode ser aproximada por

$$I_A = I(X;L_a) \approx 1 - \frac{1}{N}\sum_{k=1}^{N} \log_2\left(1+e^{-x_k L_{ak}}\right). \tag{8}$$

Se se admitir que a informação mútua média I_E também é gaussiana e consistente então

$$I_E = I(X;L_e) \approx 1 - \frac{1}{N}\sum_{k=1}^{N} \log_2\left(1+e^{-x_k L_{ek}}\right). \tag{9}$$

Esta estimativa depende da sequência de informação X. É possível, felizmente, obter uma estimativa de I_E sem conhecer X. De facto, prova-se [13] [14] que basta conhecer os valores absolutos de L_e:

$$\begin{aligned} I_E &\approx 1 - E\left[H\left(\frac{1}{1+e^{|L_e|}}\right)\right] = \\ &= 1 - \frac{1}{N}\sum_{k=1}^{N} H\left(\frac{1}{1+e^{|L_{ek}|}}\right) \end{aligned} \tag{10}$$

onde $H(\,)$ é a entropia binária[11].

O que então se tem a fazer é simular um esquema como o da Fig. 9, onde temos dois canais: o canal de comunicação propriamente dito, que produz amostras de $L(\mathbf{y}|x)$, e um canal artificial dito *extrínseco* (ou, também, *a priori*), que produz amostras de L_a. Quer $L(\mathbf{y}|x)$ quer L_a são aplicadas ao descodificador, que por sua vez produz amostras de L_e.

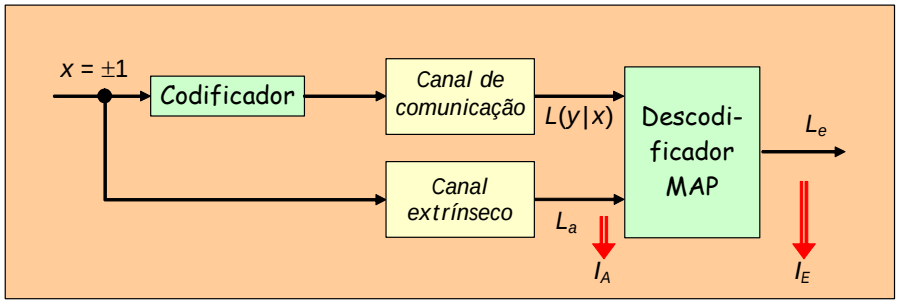

Fig. 9. Esquema geral de simulação para obter I_A e I_E a partir de L_a e L_e.

No caso do canal de comunicação ser gaussiano com ruído AWGN de média nula e variância $\sigma^2 = N_0/2E_s$ (situação retratada na Fig. 10) cada par de valores (I_A, I_E) de um descodificador é obtido realizando as seguintes operações:

[11] O expoente da Eq. (10) pode ser substituído pelo seu simétrico. Na verdade, é fácil de verificar que a entropia não se altera.

1. Gera-se uma longa sequência aleatória X de bits ±1, codifica-se e envia-se através do canal de comunicação gaussiano $\mathcal{N}(0,\sigma^2)$, obtendo-se a sequência Y de valores reais y;

   A sequência Y contém bits de informação sistemáticos e bits de paridade. Multiplicando-a por $2/\sigma^2$ *obtemos a LLR* $L(\mathbf{y}\mid x)=\frac{2}{\sigma^2}y$.

2. Faz-se atravessar X por um canal gaussiano de variância σ_a^2 (o valor médio da saída deve ser $\pm\sigma_a^2/2$);

   A sequência de saída deste canal é L_a.

3. Aplica-se L_a e $L(\mathbf{y}\mid x)$ ao descodificador e recolhe-se a informação extrínseca L_e na saída;

   Neste momento também já temos a sequência L_e.

4. Calcula-se I_A ou pela Eq. (3) ou pela Eq. (5) ou consultando uma tabela de valores (σ_a, I_A);
5. Calcula-se I_E através da Eq. (2) com integração numérica.

   Dado que não dispomos de uma expressão analítica para $p(L_e|1)$ *é preciso estimar primeiro* $p(L_e|1)$ *(construindo um histograma, por exemplo) e só depois se calcula o integral usando, por exemplo, as fórmulas do trapézio ou de Simpson (ver Apêndice A3).*

Este procedimento deve repetir-se para outros valores de σ_a^2 de modo que I_A percorra o intervalo [0,1] como na Fig. 8. É um trabalho moroso porque, para conseguirmos relevância estatística, é conveniente usar um número elevado de bits (acima de 10^4 e quanto maior melhor…) na descodificação BCJR, já de si computacionalmente demorada.

Note-se que o cálculo de I_E delineado atrás é válido para qualquer fdp $p(L_e|1)$; pelo contrário as Eqs. (9) e (10) pressupõem que $p(L_e|1)$ é gaussiana e consistente – mas, mesmo que o não seja, a estimativa de I_E é muito boa. Registe-se também que a entrada vinda do canal, $L(\mathbf{y}\mid x)=2y/\sigma^2$, é uma v.a. gaussiana de média $\pm 2/\sigma^2$ e variância $4/\sigma^2$, ou seja, é uma v.a. gaussiana consistente tal como a entrada L_a.

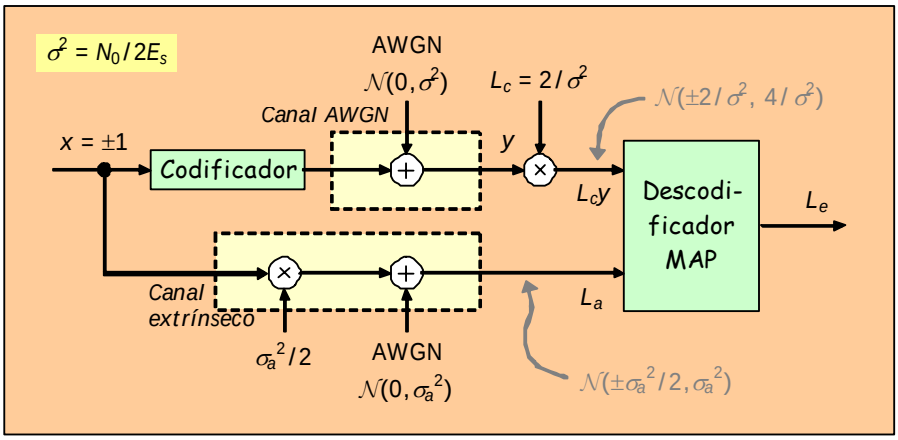

Fig. 10. Esquema de simulação em processamento turbo para se obter I_A e I_E a partir de L_a e L_e, quando o canal de comunicação é gaussiano.

Exemplo 1: Funções de transferência em descodificação turbo

Como exemplo a Fig. 11 mostra, para vários valores da relação E_b/N_0, a função de transferência, ou função EXIT, do descodificador MAP associado ao codificador convolucional recursivo e sistemático[12] de taxa 1/2 com perfuração para taxa 2/3 e matriz geradora

[12] Os codificadores convolucionais recursivos e sistemáticos são muitas vezes referidos abreviadamente como codificadores RSC, de "Recursive Systematic Convolutional [Codes]".

$$\mathbf{G} = \left[1 \quad \frac{1+D+D^2+D^3+D^4}{1+D^3+D^4}\right] = \left[1 \quad \frac{11111}{10011}\right] = \left[1 \quad \frac{37_8}{23_8}\right],$$

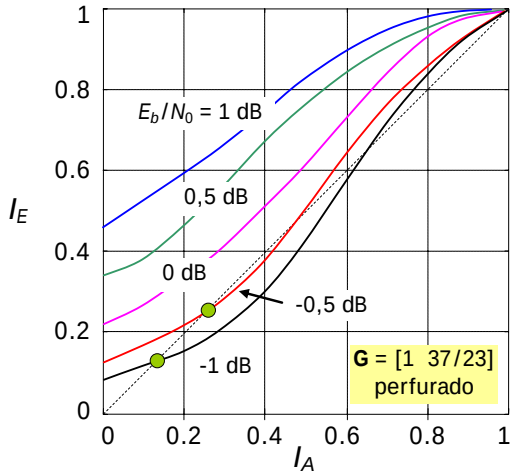

Fig. 11. Funções de transferência ou EXIT do codificador convolucional recursivo de taxa 2/3 (perfurado) com **G** = [1 37/23], para vários valores de E_b/N_0.

Foram usados N = 10 000 bits de informação (incluindo bits de cauda), a descodificação foi realizada com o algoritmo exacto log-MAP e a informação mútua média I_E foi calculada de acordo com a Eq. (2). As curvas parametrizadas por E_b/N_0 = -0,5 e -1,0 dB cruzam a diagonal do gráfico. Já sabemos que isso é indesejável.

Na Fig. 12 são apresentados os "EXIT charts" de dois turbo-códigos, um constituído pelos codificadores convolucionais do Exemplo 1 e o outro por codificadores definidos pela matriz **G** = [1 5/7].

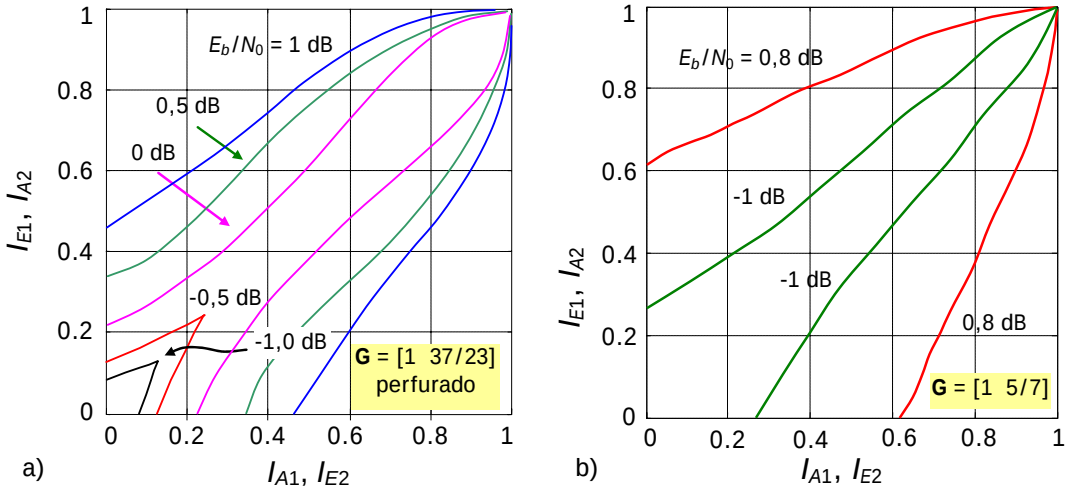

Fig. 12. a) "EXIT charts" obtidos com as funções de transferência da Fig. 11; b) "EXIT charts" correspondentes a dois codificadores convolucionais RSC iguais, com **G** = [1 5/7], E_b/N_0 = 0,8 dB e -1 dB. Número de bits de informação: 30 000.

Observamos na Fig. 12a que o *limiar de convergência* da descodificação iterativa se situa entre 0 e -0,5 dB. O limiar de convergência corresponde à situação em que as funções EXIT são tangentes e pode ser entendido como o valor de E_b/N_0 que marca a fronteira entre valer ou não valer a pena prosseguir com mais iterações para reduzir a probabilidade de erro.

Concluímos que os "EXIT charts" ajudam, de facto, a avaliar a eficiência da descodificação e, também, a projectar bons códigos e bons sistemas baseados no princípio turbo. O mesmo se passa com os códigos LDPC.

5. "EXIT Charts" de códigos LDPC

Como é sabido, um código LDPC binário é um código de blocos (n,k) caracterizado por uma matriz de verificação de paridade **H** com poucos "uns". A sua descodificação iterativa é um procedimento de transferência de mensagens entre os n nós de variáveis e os $(n-k)$ nós de paridade do seu grafo bipartido de Tanner [4]. O algoritmo de descodificação é habitualmente denominado de *algoritmo da soma-e-produto* e está fortemente aparentado com o algoritmo BCJR ou MAP da descodificação turbo. Há, basicamente, dois tipos de códigos LDPC: se cada coluna de **H** tiver o mesmo número, d_v, e cada linha tiver o mesmo número, d_c, de "uns" o código diz-se *regular*; caso contrário diz-se *irregular*. Um código LDPC regular nas condições descritas designa-se por código LDPC (d_v,d_c). A Fig. 13 apresenta um exemplo de matriz **H** de um código LDPC (2,4) juntamente com o correspondente grafo de Tanner. Neste, cada nó de variável está ligado a $d_v = 2$ nós de paridade e cada um destes está ligado a $d_c = 4$ nós de variáveis. Diz-se então que o *grau dos nós de variáveis* é d_v e que o *grau dos nós de paridade* é d_c. Os graus estão relacionados entre si através de

$$N = nd_v = (n-k)d_c\,, \tag{11}$$

em que N é o número de "uns" de **H** (ou o número de ramos do grafo de Tanner).

Pelo contrário, num código LDPC irregular os nós de variáveis e/ou de paridade têm vários graus. Por exemplo, no código LDPC da Fig. 14 sete dos dez nós de variáveis têm grau 2, dois têm grau 3 e um tem grau 4, um dos cinco nós de paridade tem grau 4 e os outros têm grau 5. Se D for o maior grau o grau médio de cada tipo de nó é dado por

$$\overline{d} = \sum_{i=1}^{D} a_i i\,,$$

em que a_i é a percentagem de nós de grau i e $\sum_{i=1}^{D} a_i = 1$, é claro.

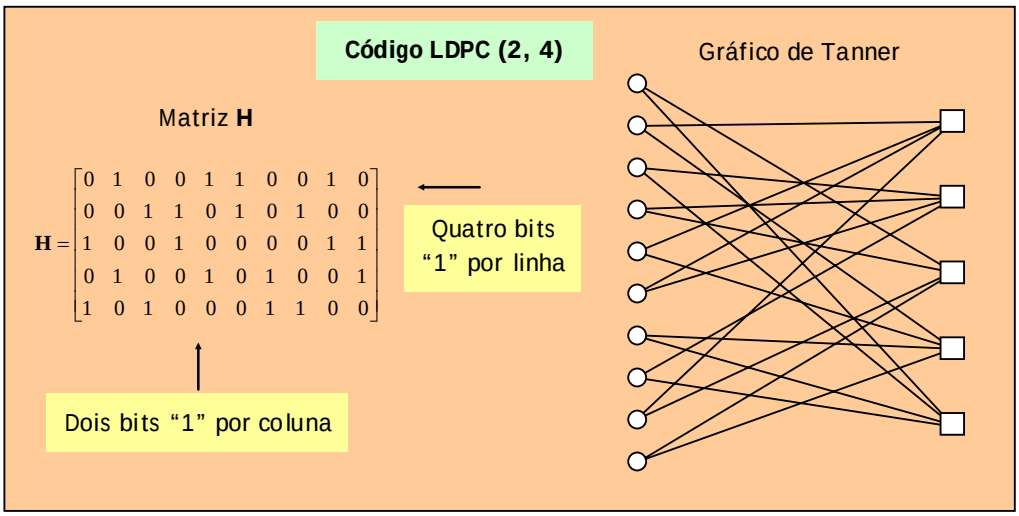

Fig. 13. Exemplo de matriz **H** e grafo de Tanner de um código LDPC regular.

Esta diferente quantidade de ramos que chegam aos nós define os *polinómios de distribuição de graus* $\lambda(x)$ e $\rho(x)$

$$\lambda(x) = \sum_i \lambda_i x^{i-1} \qquad (\text{com } \sum_i \lambda_i = 1)$$

$$\rho(x) = \sum_j \rho_j x^{j-1} \qquad (\text{com } \sum_j \rho_j = 1)$$

em que λ_i e ρ_j representam a fracção *de ramos* do grafo que estão ligados a nós de variáveis e de paridade de grau *i* e *j*, respectivamente. Assim, dos 24 ramos da Fig. 14 quatro chegam a nós de paridade de grau 4 e catorze saem de nós de variáveis de grau 2, por exemplo, ou seja, $\rho_4 = 4/24 = 1/6$ e $\lambda_2 = 14/24 = 7/12$. Portanto, no conjunto,

$$\lambda(x) = \frac{7}{12}x + \frac{1}{4}x^2 + \frac{1}{6}x^3 \qquad \rho(x) = \frac{1}{6}x^3 + \frac{5}{6}x^4 .$$

O Apêndice A5 mostra como calcular analiticamente λ_i e ρ_j a partir das percentagens de nós com o mesmo grau, e vice-versa.

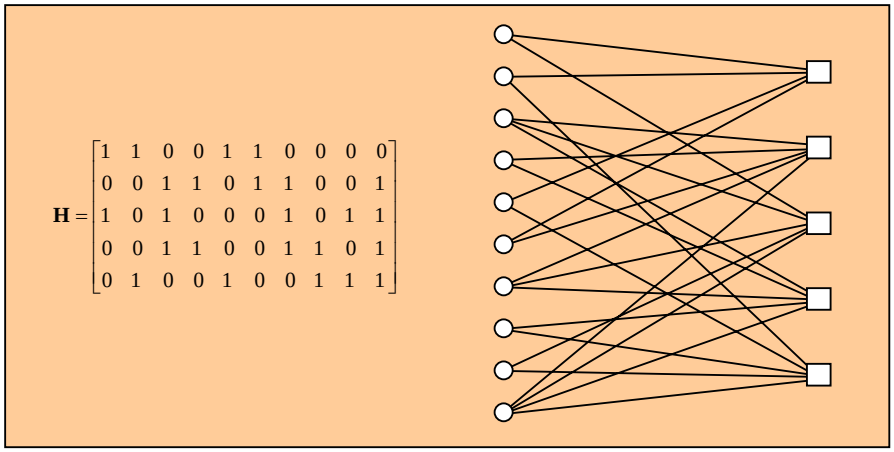

Fig. 14. Exemplo de matriz **H** e grafo de Tanner de um código LDPC irregular de tamanho $n = 10$.

A descodificação iterativa de códigos LDPC pode ser encarada como a descodificação de dois códigos concatenados em série, como na Fig. 2: o conjunto de nós de variáveis do grafo de Tanner representa o descodificador interior, o conjunto de nós de paridade representa o descodificador exterior e as linhas ou ramos que ligam os nós entre si representam as operações de entrelaçamento e desentrelaçamento [15], como se mostra na Fig. 15. Em códigos LDPC regulares (d_v,d_c) a descodificação nos nós de variáveis equivale a calcular LLRs extrínsecas num código de repetição (d_v,1) e a descodificação nos nós de paridade equivale a calcular LLRs extrínsecas num código de paridade simples (d_c, d_c - 1).

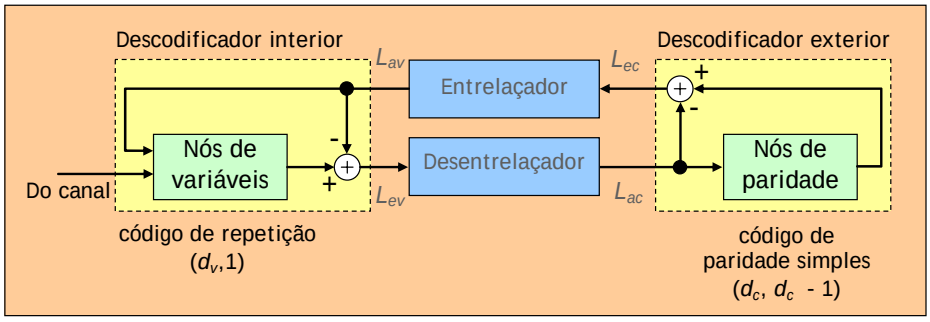

Fig. 15. Descodificador iterativo de códigos LDPC regulares.

Os "EXIT charts" de códigos LDPC são muito mais fáceis de obter que os "EXIT charts" de códigos turbo. Na verdade, ao contrário destes não é preciso fazer simulações em computador pois dispomos de expressões analíticas de cálculo das funções de transferência. Essas expressões são exactas em canais binários com rasuras, ou canais BEC, e aproximadas (mas muito aproximadas, mesmo!) em canais AWGN. É o que vamos ver em seguida.

5.1 "EXIT Charts" de códigos LDPC regulares em canais BEC

Um canal binário com rasuras (BEC) é um canal discreto sem memória caracterizado pelo diagrama de transição da Fig. 16, onde p representa a probabilidade de um bit x ser rasurado. Como é sabido, a informação mútua média entre a entrada e a saída deste canal vale $I(X;Y) = (1 - p)H[p(1)]$ e a capacidade $C_s = \max[I(X;Y)] = 1 - p$ é atingida quando os bits de entrada X são equiprováveis.

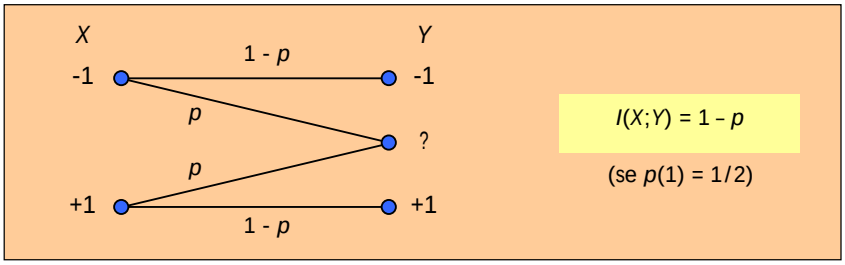

Fig. 16. O diagrama de transição de um canal BEC.

A Fig. 17 mostra os esquemas de descodificação apropriados para se determinarem as funções EXIT de códigos LDPC regulares em canais BEC [16]. Na figura "REP" e "SPC" significam "código de repetição" e "código de paridade simples"[13], respectivamente. Como se vê, no esquema de descodificação correspondente aos nós de paridade não se considera nenhum canal de comunicação pois o descodificador exterior só tem uma entrada, L_{ac}.

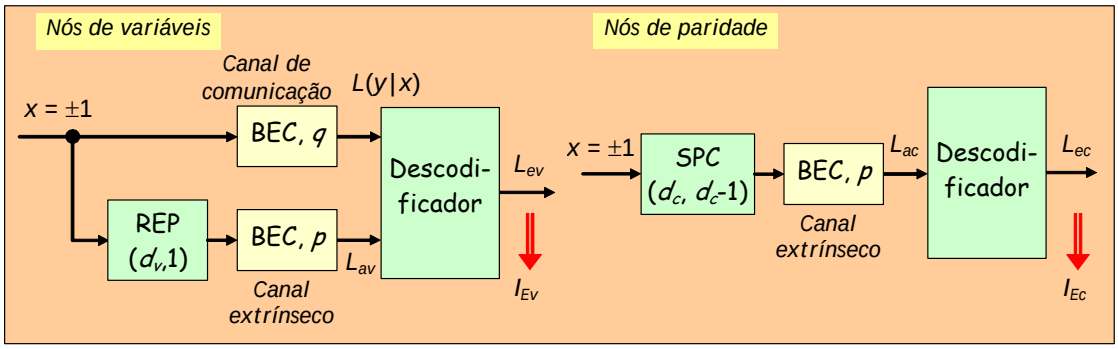

Fig. 17. Esquemas de cálculo de L_a e L_e para obtenção de funções EXIT de códigos LDPC regulares.

De acordo com [16] as várias informações mútuas médias I_A e I_E são dadas pelas expressões seguintes:

Nós de variáveis (canais BEC)

$$I_{A_v} = I(X;L_{av}) = 1-p$$
$$I_{E_v} = I(X;L_{ev}) = 1-qp^{d_v-1} \quad \Rightarrow \quad I_{E_v} = 1-q(1-I_{A_v})^{d_v-1}$$

Nós de paridade (canais BEC)

$$I_{A_c} = I(X;L_{ac}) = 1-p$$
$$I_{E_c} = I(X;L_{ec}) = (1-p)^{d_c-1} \quad \Rightarrow \quad I_{E_c} = I_{A_c}^{\,d_c-1}$$

É de notar que independentemente dos graus d_v e d_c todas as funções EXIT I_{Ev} e I_{Ec}^{-1} têm valor $1 - q$ e 0, respectivamente, no eixo das ordenadas. Note-se ainda que essas mesmas funções são linhas rectas de declives q e 1, respectivamente, quando os nós associados têm grau 2.

[13] SPC = "Single Parity Check".

Aparte: a expressão de I_{Ec} é uma manifestação da chamada *propriedade da dualidade*, que relaciona entre si as funções EXIT de códigos duais em canais BEC [15]. De facto, se os canais de comunicação e extrínseco forem canais BEC com probabilidades de rasura q e p, respectivamente, a propriedade da dualidade estabelece que

$$I_E^{\perp}(p,q) = 1 - I_E(1-p, 1-q)$$

em que $I_E^{\perp}$ e I_E representam as funções EXIT dos códigos duais $(n, n-k)$ e (n,k), respectivamente. Ora é sabido que os códigos de paridade simples e de repetição com o mesmo tamanho n são duais. Na ausência de canal de comunicação ($q = 1$) e com $n = d_v$ temos $I_{E,REP}(p) = I_{E_v} = 1 - p^{n-1}$. Portanto,

$$\begin{aligned} I_{E,SPC}(p) &= 1 - I_{E,REP}(1-p) = \\ &= 1 - \left[1 - (1-p)^{n-1}\right] = \\ &= (1-p)^{n-1} \end{aligned}$$

Considerando $I_{E_c} = I_{E,SPC}$ e $n = d_c$ e notando que $I_{A_c} = 1 - p$ obtemos $I_{E_c} = I_{A_c}^{d_c - 1}$, como já estava atrás.

A Fig. 18 apresenta "EXIT charts" de códigos LDPC regulares com $d_c = 2,4,5,6$ e $d_v = 2,3,4,5$ num canal de comunicação BEC com $q = 0,4$. Note-se que em certas combinações de graus não existe túnel de saída (por exemplo $d_v = 2$ e $d_c = 5$).

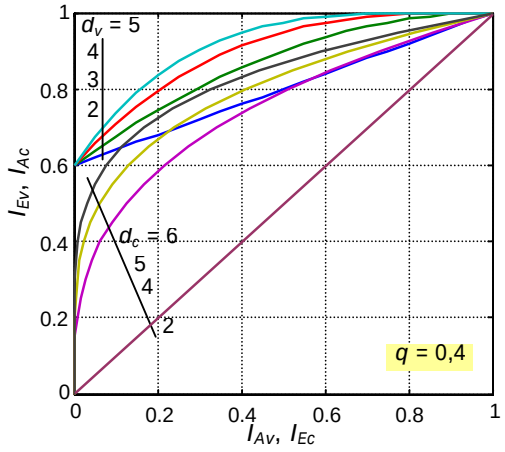

Fig. 18. "EXIT charts" de códigos LDPC regulares em canal BEC com q =0,4.

5.1.1 Cálculo analítico do limiar de convergência dos códigos LDPC regulares em canais BEC

Para que haja convergência em direcção a $I_E = 1$ é necessário que se forme um túnel de saída no "EXIT chart", como sabemos, o que obriga a que a curva EXIT dos nós de variáveis esteja sempre acima da função inversa da curva EXIT dos nós de paridade:

$$I_{E_v}(I_{A_v}) \geq I_{A_c}(I_{E_c})$$

ou

$$1 - q\left(1 - I_{A_v}\right)^{d_v - 1} \geq I_{E_c}^{1/(d_c - 1)}$$

No "EXIT chart" I_{Av} e I_{Ec} são, na realidade, a mesma abcissa. Designando-a pela letra única I reescrevemos a expressão anterior como

$$1-q\left(1-I\right)^{d_v-1} \geq I^{1/(d_c-1)},$$

onde vemos que o segundo membro (a curva de baixo, no gráfico) só depende do grau d_c. Assim, se fixarmos d_c e d_v a curva de baixo fica estática e a de cima vai descendo e aproximando-se da outra, intersectando-a mesmo, se formos aumentando a probabilidade de rasura q do canal de comunicação. Ao valor q_{lim} acima do qual as curvas se intersectam e fecham o túnel dá-se o nome de *limiar de convergência* do código LDPC. No limiar as curvas intersectam-se tangencialmente e acima dele são secantes. O ponto de tangência[14] ocorre na abcissa $I = I_{\text{lim}}$ que satisfaz a equação em x

$$\left[\left(d_c-1\right)\left(d_v-1\right)-1\right]x^{d_c-1}-\left(d_c-1\right)\left(d_v-1\right)x^{d_c-2}+1=0, \tag{12}$$

em que $x = I^{\frac{1}{d_c-1}}$, $0 \leq x \leq 1$ (ver Apêndice A4 para os pormenores). O limiar q_{lim}, esse, obtém-se depois de conhecermos I_{lim}:

$$q_{\text{lim}} = \frac{I_{\text{lim}}^{\frac{2-d_c}{d_c-1}}}{\left(d_c-1\right)\left(d_v-1\right)\left(1-I_{\text{lim}}\right)^{d_v-2}} \tag{13}$$

Em resumo: para haver convergência em canais BEC é necessário que $q \leq q_{\text{lim}}$.

Veremos adiante que se desejarmos obter um código LDPC que se aproxime da capacidade devemos procurar que a área entre curvas EXIT seja a menor possível [15]; por outras palavras, as curvas devem estar praticamente sobrepostas (ver Exemplo 6). Nesse caso, porém, o número de iterações necessário para nos aproximarmos do canto superior direito do gráfico aumenta.

Exemplo 2: limiares de convergência de códigos LDPC (3,4) e (2,4)

Seja d_v = 3 e d_c = 4. Substituindo valores na Eq. (12) obtemos a equação do 3º grau $5x^3-6x^2+1=0$, de raízes 1 e $\left(1\pm\sqrt{21}\right)/10$. Destas só nos interessa a raiz $\left(1+\sqrt{21}\right)/10$, para a qual obtemos a abcissa de tangência do "EXIT chart"

$$I_{\text{lim}} = \left(\frac{1+\sqrt{21}}{10}\right)^3 = 0{,}17398$$

(pois $I = x^{d_c-1} = x^3$). O limiar de convergência decorre imediatamente da Eq. (13):

$$q_{\text{lim}} = \frac{I_{\text{lim}}^{-2/3}}{6\left(1-I_{\text{lim}}\right)} = 0{,}64743.$$

A Fig. 19 à esquerda mostra o "EXIT chart" respectivo. Para comparação apresenta-se à direita o gráfico de um código (2,4) em canal BEC com q = 1/3. Neste caso as curvas só são tangentes no canto superior direito. Vejamos porquê. Como d_v = 2 a função EXIT dos nós de variáveis é uma recta de declive q = 1/3 e como d_c = 4 a função inferior é uma curva de derivada $1/3I_{E_c}^{-2/3}$. As duas funções são tangentes, por definição, no ponto em que ambos os declives forem iguais, o que só acontece, claro, em $I_{E_c}=1$. Se q > 1/3 as funções são secantes e fecham o túnel. Logo, q_{lim} = 1/3 nos códigos LDPC (2,4).

[14] As funções EXIT não podem ser tangentes num ponto de abcissa menor que 1 se d_v = 2 ou d_c = 2 porque, nesses casos, as funções EXIT são rectas. Para termos um ponto de tangência único terá de ser d_v > 2 e d_c > 2.

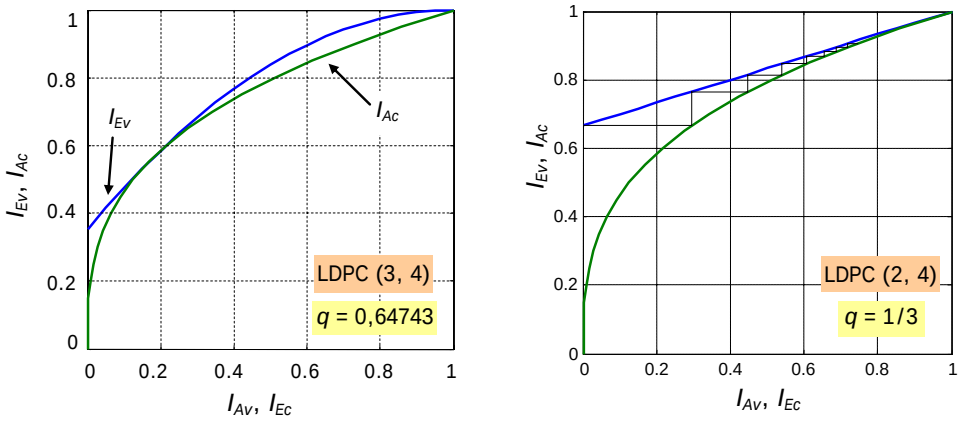

Fig. 19. "EXIT charts" dos códigos LDPC (3,4) e (2,4) nos limiares (q_{lim} =0,64743 e 1/3, respectivamente).

5.2 "EXIT Charts" de códigos LDPC regulares em canais AWGN

Agora os canais BEC da Fig. 17 são substituídos por canais AWGN. O ruído do canal de comunicação, quando este existe, tem variância

$$\sigma^2 = \frac{1}{2R_c \dfrac{E_b}{N_0}},$$

a mesma que foi usada com turbo-códigos. Tal como então, a saída desse canal deverá ser multiplicada pela medida da fiabilidade do canal $L_c = 2/\sigma^2$ para se obter a LLR $L(\mathbf{y}|x)$, que desse modo tem variância $\sigma_c^2 = \dfrac{4}{\sigma^2} = 8R_c \dfrac{E_b}{N_0}$ (ver Fig. 10 e Apêndice A2). Quanto ao canal extrínseco o ruído AWGN deve ter uma variância de $4/\sigma_a^2$ para que a variância de L_a seja σ_a^2.

A propriedade da dualidade não é exacta em canais AWGN mas é tão aproximada que também é usada neles para calcular I_{Ec}. Assim, de acordo com [16] as funções de transferência relativas aos dois tipos de nós são dadas por:

Nós de variáveis (canais AWGN)

$$I_{E_v}(I_{A_v}, d_v, E_b/N_0, R_c) = J\left(\sqrt{(d_v - 1)\left[J^{-1}(I_{A_v})\right]^2 + \sigma_c^2}\right)$$

Nós de paridade (canais AWGN)

$$I_{E_c}(I_{A_c}, d_c) \approx 1 - J\left(\sqrt{(d_c - 1)}\, J^{-1}(1 - I_{A_c})\right)$$

Para o traçado dos "EXIT charts" pode interessar-nos conhecer a função inversa[15]:

$$I_{A_c}(I_{E_c}, d_c) \approx 1 - J\left(\frac{J^{-1}(1 - I_{E_c})}{\sqrt{(d_c - 1)}}\right).$$

[15] Se o traçado do gráfico EXIT for feito em Matlab ou noutra ferramenta similar não é necessário calcular a função inversa (basta trocar a ordem de certos argumentos nas chamadas de funções gráficas como *plot*).

Recorda-se que a função $I_A = J(\sigma_a)$ foi anteriormente definida na Eq. (4) e aproximada pela Eq. (5) e a sua inversa aproximada pela Eq. (6). Observando a expressão de I_{Ev} constatamos que para $I_{Ac} = 0$ é sempre $I_{E_v}(0, d_v, E_b/N_0, R_c) = J(\sigma_c)$ independentemente dos outros parâmetros de entrada.

Aparte: vejamos como se obteve I_{Ec} aplicando a propriedade da dualidade: como, para I_{Ec}, não há canal de comunicação (Fig. 17 à direita) $\sigma_c^2 = 0$ na expressão de I_{Ev} e, portanto,

$$I_{E_c}(I_{A_c}, d_c) \approx 1 - I_{E_v}(1 - I_{A_c}, d_c) = \\ = 1 - J\left(\sqrt{(d_c - 1)} J^{-1}(1 - I_{A_c})\right)$$

A Fig. 20 mostra as funções EXIT de códigos LDPC regulares de taxa 1/2 com d_v e d_c iguais a 2, 3, 4, 6 e 8 num canal de comunicação AWGN em que E_b/N_0=1 dB (note-se o ponto de partida comum de todas as curvas I_{Ev}: $J(\sigma_c) = J(2, 24) = 0{,}56$). A Fig. 21 apresenta os "EXIT charts" correspondentes mas considerando apenas $d_c = 8$. Verificamos aí que não há túneis de saída se $d_v = 2$, 3 ou 4.

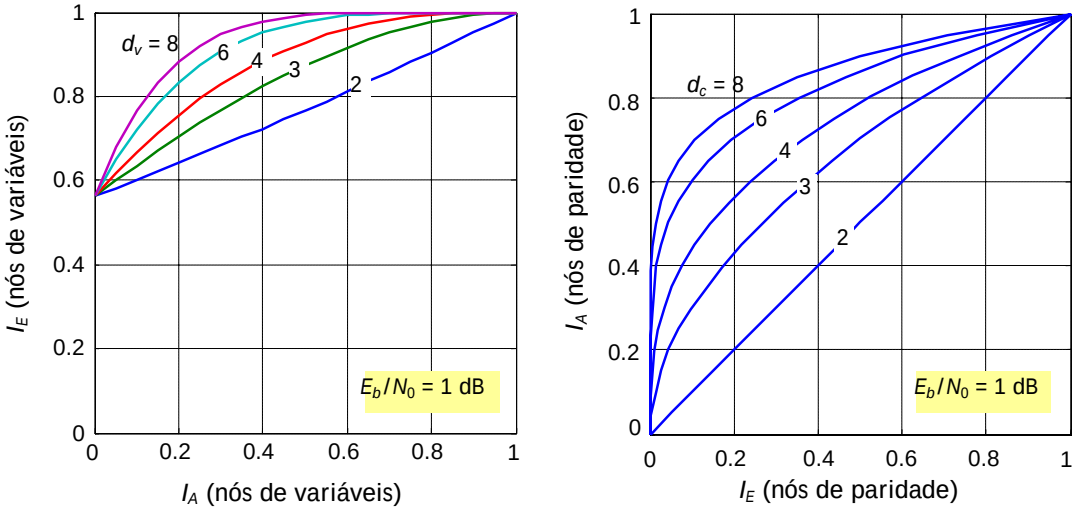

Fig. 20. Funções EXIT de vários códigos LDPC regulares de taxa 1/2, com E_b/N_0=1 dB em canal AWGN.

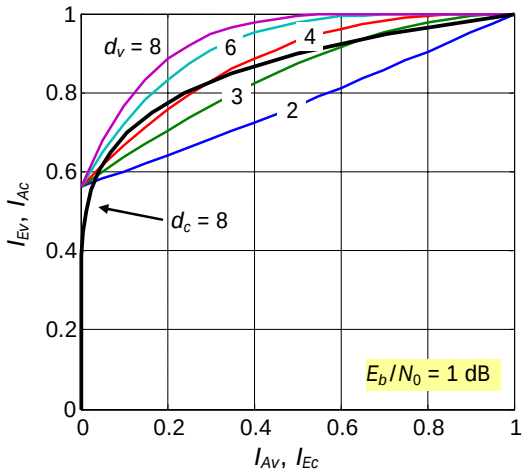

Fig. 21. "EXIT charts" de códigos LDPC regulares de taxa 1/2, de diferentes graus de variáveis e d_c = 8, em canal AWGN com E_b/N_0=1 dB.

5.3 "EXIT Charts" de códigos LDPC irregulares

Num código LDPC irregular o número de ramos do grafo de Tanner ligados a cada nó não é o mesmo. Nesses códigos a função EXIT de um grupo de nós (de variáveis ou de paridade) é a média das funções EXIT associadas a cada grau ponderada pelas proporções dos ramos ligados aos nós desse grau. Assim, suponhamos que temos um código LDPC irregular em que num dos grupos de nós o grau máximo é D. Se b_i representar a fracção dos ramos que incidem nos nós de grau i a informação mútua média I_E é igual à média ponderada das informações mútuas médias I_{Ei} associadas aos nós de grau i [15] [16]:

$$I_E = \sum_{i=1}^{D} b_i I_{E_i} \,, \tag{14}$$

em que $\sum_{i=1}^{D} b_i = 1$. Se os nós de variáveis e de paridade tiverem graus máximos D_v e D_c, respectivamente, e os coeficientes dos polinómios de distribuição de graus $\lambda(x)$ e $\rho(x)$ forem, como antes, λ_i e ρ_j (correspondem, é claro, às fracções genéricas b_i) as funções EXIT de tais códigos irregulares em canais BEC e AWGN são expressas pelas fórmulas apresentadas em seguida.

5.3.1 Canais BEC

No caso dos canais BEC é fácil de concluir das fórmulas da Sec. 5.1 e da Eq. (14) que, com $I_A = 1 - p$,

Nós de variáveis (LDPC irregulares e canais BEC)

$$I_{E_v} = 1 - q\sum_{i=1}^{D_v} \lambda_i p^{i-1} = 1 - q\lambda(p) \quad \Rightarrow \quad I_{E_v} = 1 - q\lambda(1 - I_{A_v})$$

Nós de paridade (LDPC irregulares e canais BEC)

$$I_{E_c} = \sum_{j=1}^{D_c} \rho_j (1-p)^{j-1} = \rho(1-p) \quad \Rightarrow \quad I_{E_c} = \rho(I_{A_c})$$

Exemplo 3: Funções EXIT e "EXIT chart" de um código LDPC irregular em canal BEC

Admitamos, por exemplo, que num certo código LDPC 30% dos ramos que incidem nos nós de variáveis têm grau 2, 20% têm grau 3 e os restantes 50% têm grau 4 e que, no caso dos nós de paridade, 60% dos ramos correspondem a grau 4 e 40% a grau 6. Portanto, o grau máximo dos nós de variáveis é $D_v = 4$ e os coeficientes de $\lambda(x)$ são $\lambda_2 = 0{,}3$, $\lambda_3 = 0{,}2$ e $\lambda_4 = 0{,}5$, ou seja, $\lambda(x) = 0{,}3x + 0{,}2x^2 + 0{,}5x^3$; do mesmo modo, $D_c = 6$ e $\rho(x) = 0{,}6x^3 + 0{,}4x^5$. Se os canais de comunicação e extrínseco forem BEC com probabilidades de rasura q e p, respectivamente, a função EXIT dos nós de variáveis é igual a

$$\begin{aligned} I_{E_v} &= 1 - q\lambda(p) = \\ &= 1 - q\left(0{,}3p + 0{,}2p^2 + 0{,}5p^3\right) \end{aligned}$$

ou $I_{E_v} = 1 - q\left(1 - 2{,}2I_{A_v} + 1{,}7I_{A_v}^2 - 0{,}5I_{A_v}^3\right)$, e a função EXIT dos nós de paridade é igual a $I_{E_c} = \rho(1-p) = 0{,}6(1-p)^3 + 0{,}4(1-p)^5$, ou $I_{E_c} = \rho(I_{A_c}) = 0{,}6I_{A_c}^3 + 0{,}4I_{A_c}^5$. O "EXIT chart" respectivo para q = 0,4 é apresentado na Fig. 22.

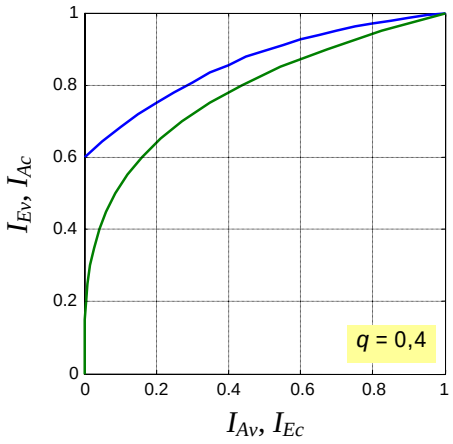

Fig. 22. "EXIT chart" de um código LDPC irregular definido pelos polinómios $\lambda(x) = 0,3x + 0,2x^2 + 0,5x^3$ e $\rho(x) = 0,6x^3 + 0,4x^5$ em canal BEC com q = 0,4.

5.3.1.1 *Optimização de códigos LDPC*

Seja A_v e A_c as áreas por baixo das funções EXIT dos nós de variáveis, $I_{E_v} = T_1(I_{A_v})$, e de paridade, $I_{E_c} = T_2(I_{A_c})$, respectivamente. Para que haja um túnel de convergência no "EXIT chart" o gráfico da função I_{E_v} tem de estar sempre acima do gráfico de $I_{A_c} = T_2^{-1}(I_{E_c})$ pelo que a área A_v tem de ser maior que a área 1 - A_c. Com códigos LDPC regulares essas áreas são iguais a

$$A_v = \int_0^1 I_{E_v} dI_{A_v} = \int_0^1 1 - q\left(1 - I_{A_v}\right)^{d_v - 1} dI_{A_v} = \\ = 1 - \frac{q}{d_v} \tag{15}$$

$$1 - A_c = 1 - \int_0^1 I_{E_c} dI_{A_c} = 1 - \int_0^1 I_{A_c}^{\,d_c - 1} dI_{A_c} = \\ = 1 - \frac{1}{d_c} \tag{16}$$[16]

Portanto, se $A_v > 1 - A_c$, então $1 - \frac{q}{d_v} > 1 - \frac{1}{d_c}$, ou seja, $q < \frac{d_v}{d_c}$. Mas como $C_s = 1 - q$ é a capacidade do canal BEC, em bits/símbolo, como se viu já, e $d_v / d_c = 1 - R_c$ (cf. Eqs. (11) e (28)), terá de ser $1 - C_s < 1 - R_c$, ou $R_c < C_s$. Isto é… afinal… o famoso *Teorema da Codificação de Canal*, de Claude Shannon, aqui visualmente manifestado.

A área do túnel de saída é igual a

$$\Delta A = A_v - (1 - A_c) = 1 - \frac{q}{d_v} - \left(1 - \frac{1}{d_c}\right) = \frac{C_s - R_c}{d_v}$$

Desta expressão extraímos uma conclusão muito importante e útil para o projecto de códigos LDPC: se nos quisermos aproximar da capacidade do canal, isto é, se desejarmos $R_c \to C_s$, então $\Delta A \to 0$ e o túnel de saída

[16] Como se vê, a área de baixo, $1 - A_c = (d_c - 1)/d_c$, é igual à taxa do seu código de paridade simples (d_c, d_c - 1).

deve ser o mais estreito possível. A esta conclusão de que a área do túnel corresponde a uma *perda* em termos de taxa do código dá-se o nome de *propriedade da área*.

Em códigos LDPC irregulares a conjugação das Eqs. (14), (15), (16) e as relações do Apêndice A5 conduzem a equações semelhantes, onde os graus de nós são substituídos por graus médios, e a conclusão é a mesma: o túnel deve ser estreitinho.

$$A_v = 1 - \frac{q}{\bar{d}_v} \qquad 1 - A_c = 1 - \frac{1}{\bar{d}_c} \qquad \Delta A = A_v - (1 - A_c) = \frac{C_s - R_c}{\bar{d}_v}.$$

A utilização de nós com diferentes graus permite mais liberdade de escolha e torna mais flexível o ajuste das curvas EXIT uma à outra, tarefa habilidosa que consiste em "jogar" adequadamente com os coeficientes dos polinómios $\lambda(x)$ e $\rho(x)$.

Exemplo 4: "EXIT chart" de código LDPC com curvas ajustadas através de série de Taylor

Uma das maneiras de ajustar as curvas EXIT uma à outra para diminuir a área entre elas passa por representar uma das curvas por uma série de Taylor e ajustar a outra ao polinómio resultante, tendo presente que a função EXIT dos nós de variáveis tem de estar sempre acima da outra curva, sem intersecção. Como exemplo simples vamos supor que os nós de paridade têm todos o mesmo grau, 5, e que queremos obter adequados coeficientes de $\lambda(x)$.

Com d_c = 5 temos $I_{E_c} = (1-p)^4$ e $I_{E_c}^{-1} = (1-p)^{1/4}$. A representação desta função inversa em série de Taylor na abcissa p = 0 (isto é, em A_c = 1) – série de McLaurin, portanto – é

$$I_{E_c}^{-1} = (1-p)^{1/4} = \\ = 1 - \frac{1}{4}p - \frac{3}{32}p^2 - \frac{7}{128}p^3 - \frac{77}{2048}p^4 - \ldots$$

Todos os termos restantes da série diminuem a função $I_{E_c}^{-1}$ pelo que podemos escrever que $1 - \frac{1}{4}p - \frac{3}{32}p^2 - \frac{7}{128}p^3 - \frac{77}{2048}p^4 > I_{E_c}^{-1}$. Logo, se tomarmos $I_{E_v} = 1 - \frac{1}{4}p - \frac{3}{32}p^2 - \frac{7}{128}p^3 - \frac{77}{2048}p^4$ estamos a garantir que $I_{E_v} > I_{E_c}^{-1}$ para qualquer abcissa I_A, como queremos para que as curvas não se cruzem. Mas $I_{E_v} = 1 - q\sum_{i=1}^{D_v} \lambda_i p^{i-1}$. Então, pondo em evidência $\frac{1}{4} + \frac{3}{32} + \frac{7}{128} + \frac{77}{2048} = \frac{893}{2048}$ escrevemos

$$I_{E_v} = 1 - \frac{893}{2048}\left(\frac{512}{893}p + \frac{192}{893}p^2 + \frac{112}{893}p^3 + \frac{77}{893}p^4\right)$$

e identificamos a probabilidade de rasura $q = \frac{893}{2048}$ e os coeficientes $\lambda_2 = \frac{512}{893}$, $\lambda_3 = \frac{192}{893}$, $\lambda_4 = \frac{112}{893}$ e $\lambda_5 = \frac{77}{893}$ (claro que $\sum_{i=2}^{5} \lambda_i = 1$). A capacidade do canal BEC é C_s = 1 – q = 0,5640 bits/símbolo. O grau médio dos nós de variáveis é $\bar{d}_v = 2{,}46$ e a taxa do código é $R_c = 1 - \bar{d}_v / d_c = 0{,}5085$, valor que está longe de C_s e revela que ainda há muita margem para melhoria. Na verdade, observando na Fig. 23 o "EXIT chart" constatamos que só tomar os menores graus (neste caso 2, 3, 4 e 5) pode não conduzir ao melhor ajuste de curvas (isso é nítido na região de valores baixos de I_A). No Exemplo 6, pelo contrário, é apresentado o "EXIT chart" de um código irregular mais bem ajustado, em que os graus de variáveis são mais díspares (2, 3, 4 e 10) e há dois graus de nós de paridade em vez de um só.

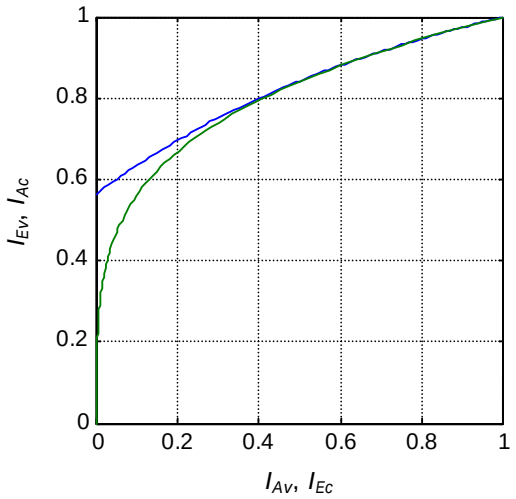

Fig. 23. "EXIT chart" de um código LDPC irregular com λ_2 = 512/893, λ_3 = 192/893, λ_4 = 112/893, λ_5 = 77/893 e d_c = 5 em canal BEC com q = 893/2048.

5.3.2 Canais AWGN

Em canais AWGN as funções EXIT são obtidas das fórmulas da Sec. 5.1.1 e da Eq. (14):

Nós de variáveis (LDPC irregulares e canais AWGN)

$$I_{E_v} = \sum_{i=1}^{D_v} \lambda_i J\left(\sqrt{(i-1)\left[J^{-1}(I_{A_v})\right]^2 + \sigma_c^2}\right)$$

Nós de paridade (LDPC irregulares e canais AWGN)

$$I_{E_c} \approx \sum_{j=1}^{D_c} \rho_j \left[1 - J\left(\sqrt{(j-1)}J^{-1}(1-I_{A_c})\right)\right]$$

Exemplo 5: Funções EXIT e "EXIT chart" de um código LDPC irregular em canal AWGN

Tomemos como exemplo o código LDPC irregular da Fig. 14, cujos polinómios de distribuição de grau são, como vimos, $\lambda(x) = \frac{7}{12}x + \frac{1}{4}x^2 + \frac{1}{6}x^3$ e $\rho(x) = \frac{1}{6}x^3 + \frac{5}{6}x^4$ e, portanto, λ_2 = 7/12, λ_3 = 1/4, λ_4 = 1/6, ρ_4 = 1/6 e ρ_5 = 5/6. As funções EXIT que lhes correspondem são

$$I_{E_v} = \frac{7}{12}J\left(\sqrt{\left[J^{-1}(I_{A_v})\right]^2 + \sigma_c^2}\right) + \frac{1}{4}J\left(\sqrt{2\left[J^{-1}(I_{A_v})\right]^2 + \sigma_c^2}\right) + \frac{1}{6}J\left(\sqrt{3\left[J^{-1}(I_{A_v})\right]^2 + \sigma_c^2}\right) =$$
$$= \frac{7}{12}J\left(\sqrt{\sigma_a^2 + \sigma_c^2}\right) + \frac{1}{4}J\left(\sqrt{2\sigma_a^2 + \sigma_c^2}\right) + \frac{1}{6}J\left(\sqrt{3\sigma_a^2 + \sigma_c^2}\right)$$

$$I_{E_c} \approx \frac{1}{6}\left[1 - J\left(\sqrt{3}J^{-1}(1-I_{A_c})\right)\right] + \frac{5}{6}\left[1 - J\left(2J^{-1}(1-I_{A_c})\right)\right]$$

onde, para simplificar a escrita, se considerou $\sigma_a = J^{-1}\left(I_{A_v}\right)$. A Fig. 24 apresenta as cinco funções EXIT individuais e o "EXIT chart" resultante das médias, se E_b/N_0 = 2 dB.

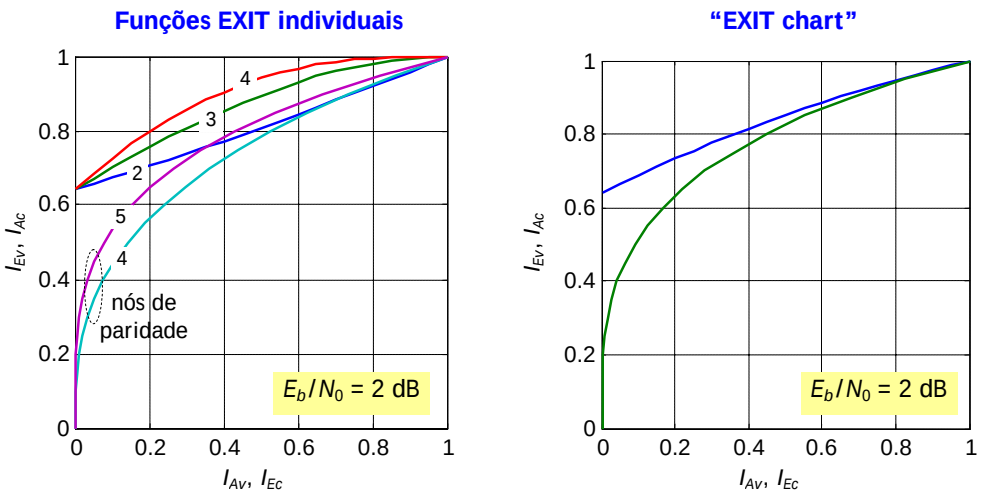

Fig. 24. "EXIT chart" de um código LDPC irregular com $\lambda_2 = 7/12$, $\lambda_3 = 1/4$, $\lambda_4 = 1/6$, $\rho_4 = 1/6$ e $\rho_5 = 5/6$ em canal AWGN com $E_b/N_0 = 2$ dB.

Exemplo 6: "EXIT chart" de um código LDPC irregular optimizado (canal AWGN)

Disse-se atrás que para optimizar um código LDPC (no sentido da aproximação à capacidade) deve procurar-se que o túnel de saída do "EXIT chart" seja o mais estreito possível. Imagina-se, certamente, que esta tarefa não é fácil. A Fig. 25 apresenta um exemplo, retirado do livro de Schlegel e Perez [17], de um código optimizado para um canal AWGN (tendo-se considerado E_b/N_0 = 0,7 dB). Os graus dos nós estão assim distribuídos pelos ramos do grafo de Tanner:

$$\lambda_2 = 0,25105 \quad \lambda_3 = 0,30938 \quad \lambda_4 = 0,00104 \quad \lambda_{10} = 0,43853 \quad \rho_7 = 0,63676 \quad \rho_8 = 0,36324$$

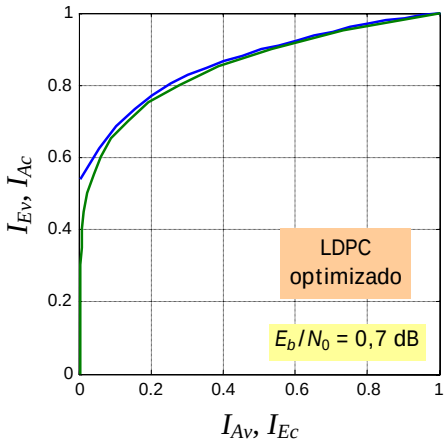

Fig. 25. "EXIT chart" de um código LDPC irregular optimizado. Canal AWGN com E_b/N_0 = 0,7 dB.

6. Apêndice A1
Algumas propriedades das funções densidade de probabilidade

Em seguida vão ser revistas algumas propriedades das funções densidade de probabilidade que têm importância para os "EXIT charts", nomeadamente com códigos turbo e quando as variáveis aleatórias envolvidas são gaussianas.

Na Fig. 26 X e Y são os sinais de entrada e saída de um canal de comunicações genérico. Este pode representar quer um canal contínuo, com entradas contínuas ou discretas e saídas contínuas, quer um canal discreto, com entradas e saídas discretas. Na figura estão também indicadas as probabilidades ou as funções densidade de probabilidade (fdp), consoante o contexto, das variáveis aleatórias envolvidas. No caso de variáveis binárias X de valores $x = \pm 1$ usaremos frequentemente as notações simplificadas $p(x = \pm 1) = p(\pm 1)$ e $p(y|x = \pm 1) = p(y|\pm 1)$. A $p(y|x)$ dá-se por vezes o nome de *verosimilhança*.

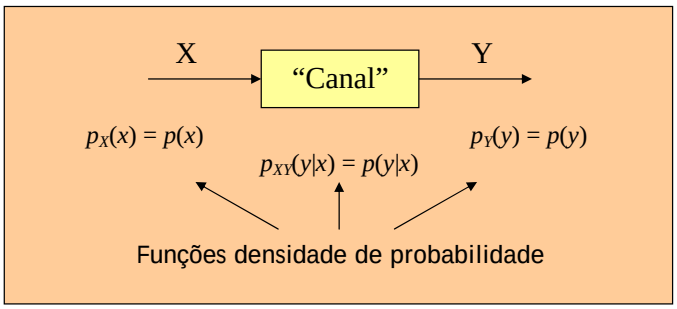

Fig. 26. As entradas e saídas de um canal genérico e as suas probabilidades e funções densidade de probabilidade

6.1 Funções densidade de probabilidade simétricas

Suponhamos que as fdps condicionais $p(y|\text{-}1)$ e $p(y|1)$ têm médias simétricas -μ e μ, respectivamente. Se cada uma das fdps for simétrica em relação ao seu valor médio então

$$p(y\,|\,-1) = p(-y\,|\,1) \tag{17}$$

6.2 Funções densidade de probabilidade consistentes

De acordo com a definição de [18] uma fdp $p(y)$ diz-se *consistente* se

$$p(y) = p(-y)e^{y} \tag{18}$$

ou, equivalentemente, se $y = \ln\left[p(y)/p(-y)\right]$.

6.2.1 Funções densidade de probabilidade gaussianas consistentes

Uma variável aleatória gaussiana Y de média μ e variância σ^2, designada habitualmente por $Y \sim \mathcal{N}(\mu,\sigma^2)$, é descrita pela fdp $p(y) = \dfrac{1}{\sqrt{2\pi\sigma^2}}\exp\left[-(y-\mu)^2/2\sigma^2\right]$. Se esta fdp gaussiana for consistente então o valor médio μ é metade da variância, $\mu = \sigma^2/2$. De facto, se calcularmos a razão $p(y)/p(-y)$,

$$\frac{p(y)}{p(-y)} = \frac{\dfrac{1}{\sqrt{2\pi\sigma^2}}\exp\left(-(y-\mu)^2/2\sigma^2\right)}{\dfrac{1}{\sqrt{2\pi\sigma^2}}\exp\left(-(-y-\mu)^2/2\sigma^2\right)} = e^{2\mu y/\sigma^2},$$

e impusermos a *condição de consistência* referida, $p(y) = p(-y)e^{y}$, então terá de ser $2\mu/\sigma^2 = 1$, ou $\mu = \sigma^2/2$, *c.q.d.*

Uma variável aleatória gaussiana e consistente, $Y \sim \mathcal{N}(\sigma^2/2,\sigma^2)$ é caracterizada, portanto, por um único parâmetro.

7. Apêndice A2
LLRs condicionais

Neste Apêndice é mostrado como as LLR condicionais $L(x|y)$ e $L(y|x)$ estão relacionadas entre si.

O teorema de Bayes diz-nos que

$$p(x \mid y) = \frac{p(y \mid x)\, p(x)}{p(y)}$$

Com variável binária X de valores $x = \pm 1$ o quociente $\dfrac{p(x=1 \mid y)}{p(x=-1 \mid y)}$ é igual a

$$\frac{p(x=1 \mid y)}{p(x=-1 \mid y)} = \frac{p(y \mid x=1)\, p(x=1)}{p(y \mid x=-1)\, p(x=-1)}$$

Aplicando logaritmos a este quociente obtemos a *LLR condicional a posteriori* $L(x|y)$:

$$L(x \mid y) = \ln \frac{p(x=1 \mid y)}{p(x=-1 \mid y)} = \underbrace{\ln \frac{p(y \mid x=1)}{p(y \mid x=-1)}}_{L(y|x)} + \underbrace{\ln \frac{p(x=1)}{p(x=-1)}}_{L_a(x)}$$

Ou seja[17]:

$$L(x \mid y) = L(y \mid x) + L_a(x) \tag{19}$$

A quantidade $L_a(x) = \ln \dfrac{p(x=1)}{p(x=-1)}$ é a LLR *a priori*. Quanto a $L(y|x)$, se, como na Fig. 27, as fdps $p(y|x = \pm 1)$ forem gaussianas, $\mathcal{N}(\pm\mu, \sigma^2)$, a razão de verosimilhanças é igual a

$$\frac{p(y|1)}{p(y|-1)} = \frac{\dfrac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-(y-\mu)^2 / 2\sigma^2\right)}{\dfrac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-(y+\mu)^2 / 2\sigma^2\right)} = e^{2\mu y/\sigma^2} \tag{20}$$

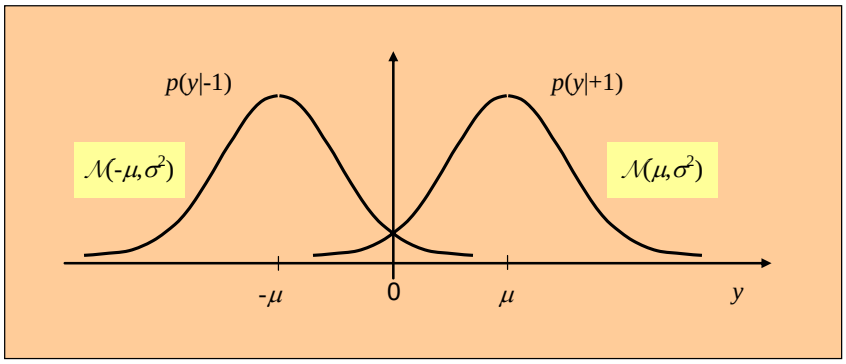

Fig. 27. Duas funções densidade de probabilidade gaussianas de valores médios simétricos e igual variância.

[17] Não confundir esta expressão geral com a expressão particular $L(x \mid \mathbf{y}) = L_e(x) + L(\mathbf{y} \mid x) + L_a(x)$ (ver Secção 2), obtida com uma sequência recebida **y** proveniente de um codificador *sistemático*.

Definindo $L_c = 2\mu/\sigma^2$ e aplicando logaritmos obtemos

$$L(y\,|\,x) = \ln\frac{p(y\,|\,1)}{p(y\,|\,-1)} = L_c\,y$$

pelo que, da Eq. (19),

$$L(x\,|\,y) = L_c\,y + L_a(x)\,.$$

O valor médio e o desvio-padrão de $L(y\,|\,x) = L_c\,y$ são iguais, respectivamente, ao produto do valor médio e do desvio-padrão de *Y* por L_c. Como tal, a variância de $L(y\,|\,x)$ é igual a

$$\sigma_c^2 = \sigma^2 L_c^2 = \frac{4\mu^2}{\sigma^2}$$

e o valor médio é metade, ou seja, $L(y\,|\,x)$ é uma v.a. gaussiana e consistente $\mathcal{N}(\pm\sigma_c^2/2, \sigma_c^2)$.

Note-se que para $x = \pm 1$ a Eq. (20), $\dfrac{p(y|1)}{p(y|-1)} = e^{L_c y}$, pode ser escrita como

$$\frac{p(y|x)}{p(y|-x)} = e^{L_c xy}$$

a qual, tendo em conta a simetria das fdps gaussianas – ou seja, que $p(y\,|\,-1) = p(-y\,|\,1)$ [cf. Eq. (17)] – é equivalente a

$$\frac{p(y|x)}{p(-y|x)} = e^{L_c xy}\,.$$

Mostra-se em [3] que $L_c = 2\mu/\sigma^2$ é também igual a

$$L_c = 2\mu\frac{E_s}{N_0/2} = 4\mu\frac{E_s}{N_0} \qquad \left(\overset{\mu=1}{\Rightarrow} \quad L_c = \frac{4E_s}{N_0}\right)$$

em que E_s é a energia do bit transmitido (ou seja, energia do bit codificado) e $N_0/2$ é a densidade espectral de potência do ruído AWGN à saída do filtro adaptado do receptor. O parâmetro L_c é chamado por uns *medida da fiabilidade do canal* e por outros *informação sobre o estado do canal* ("Channel State Information").

8. Apêndice A3
Informação mútua média: revisão de expressões

Neste Apêndice são apresentadas as diversas definições da informação mútua média associada ao canal da Fig. 26. Nuns casos todas as variáveis envolvidas são discretas, noutros são contínuas e noutros ainda são discretas e contínuas. De notar que nas expressões seguintes x_i representa um valor possível da v.a. discreta *X* (que pode ser binária ou não), ao contrário da Eq. (9), por exemplo, onde o símbolo x_k representa o *k*-ésimo bit de uma sequência binária *X*.

Pode, é claro, usar-se a definição genérica

$$I(X;Y) = H(X) - H(X\,|\,Y) = H(Y) - H(Y\,|\,X)\,,$$

em que X e Y são as v.a. da Fig. 26, $H(X)$ e $H(Y)$ são as entropias de X e Y, respectivamente, e $H(X|Y)$ e $H(Y|X)$ são entropias condicionais. Recorda-se que com variáveis discretas se tem, por exemplo,

$$H(X) = H\left[p(x_1), p(x_2),\ldots\right] = -\sum_i p(x_i)\log_2 p(x_i)$$

$$H(Y \mid X) = -\sum_i \sum_j p(x_i, y_j)\log_2 p(y_j \mid x_i)$$

e com variáveis contínuas

$$H(X) = -\int_{-\infty}^{\infty} p(x)\log_2 p(x)dx$$

$$H(Y \mid X) = -\iint p(x, y)\log_2 p(y \mid x)dxdy$$

8.1 Informação mútua média com fontes e canais discretos

X e *Y*: variáveis aleatórias discretas

$$I(X;Y) = \sum_i \sum_j p(x_i, y_j) I(x_i; y_j) = \sum_i \sum_j p(x_i, y_j)\log_2 \frac{p(x_i, y_j)}{p(x_i)p(y_j)} =$$
$$= \sum_i \sum_j p(x_i)p(y_j|x_i)\log_2 \frac{p(y_j|x_i)}{p(y_j)}$$

em que $p(y_j) = \sum_i p(x_i)p(y_j \mid x_i)$.

8.2 Informação mútua média com fontes e canais contínuos

X e *Y*: variáveis aleatórias contínuas

$$I(X;Y) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} p(x,y)\log_2 \frac{p(x,y)}{p(x)p(y)}dxdy = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} p(x)p(y|x)\log_2 \frac{p(y|x)}{p(y)}dxdy$$

8.3 Informação mútua média com fontes discretas e canais contínuos

X: v.a. discreta; *Y*: v.a. contínua

A variável discreta X pode tomar M valores x_i, $i = 1,2,\ldots,M$.

$$I(X;Y) = \sum_{i=1}^{M}\int_{-\infty}^{\infty} p(x_i)p(y|x_i)\log_2 \frac{p(y|x_i)}{p(y)}dy \qquad (21)$$

Se os valores, ou símbolos, X forem equiprováveis: $I(X;Y) = \frac{1}{M}\sum_{i=1}^{M}\int_{-\infty}^{\infty} p(y|x_i)\log_2 \frac{p(y|x_i)}{p(y)}dy$.

8.3.1 Caso particular: símbolos X binários equiprováveis

Seja $X \in \{\pm 1\}$ e $p(x = \pm 1) = p(\pm 1) = 1/2$. Neste caso a Eq. (21) escreve-se

$$I(X;Y) = \frac{1}{2} \sum_{x\in\{\pm 1\}} \int_{-\infty}^{\infty} p(y|x) \log_2 \frac{p(y|x)}{p(y)} dy$$

Mas

$$p(y) = \sum_{i=1}^{2} p(x_i)\, p(y \mid x_i) =$$

$$= p(-1)\, p(y \mid -1) + p(1)\, p(y \mid 1) = \frac{1}{2}\left[p(y \mid -1) + p(y \mid 1) \right]$$

Logo,

$$I(X;Y) = \frac{1}{2} \sum_{x\in\{\pm 1\}} \int_{-\infty}^{\infty} p(y|x) \log_2 \frac{2\, p(y|x)}{p(y|-1) + p(y|1)} dy \tag{22}$$

Se as fdps $p(y|\pm 1)$ tiverem valores médios $\pm\mu$ e forem simétricas relativamente a esses valores médios a expressão anterior pode ser simplificada. De facto, desenvolvendo a função integranda obtemos

$$I(X;Y) = \frac{1}{2} \sum_{x\in\{\pm 1\}} \left\{ \underbrace{\int_{-\infty}^{\infty} p(y|x) \log_2 2 dy}_{1} + \int_{-\infty}^{\infty} p(y|x) \log_2 \frac{p(y|x)}{p(y|-1) + p(y|1)} dy \right\} =$$

$$= \frac{1}{2} \left\{ 2 + \int_{-\infty}^{\infty} p(y|-1) \log_2 \frac{p(y|-1)}{p(y|-1) + p(y|1)} dy + \int_{-\infty}^{\infty} p(y|1) \log_2 \frac{p(y|1)}{p(y|-1) + p(y|1)} dy \right\}$$

Se agora usarmos a Eq. (17), válida para fdps simétricas, concluiremos que os integrais são iguais. Continuando o desenvolvimento chegamos à expressão simplificada

$$I(X;Y) = 1 - \int_{-\infty}^{\infty} p(y|1) \log_2 \left[1 + \frac{p(y|-1)}{p(y|1)} \right] dy \tag{23}$$

Se além de simétricas as fdps $p(y|\pm 1)$ forem gaussianas, $\mathcal{N}(\pm\mu, \sigma^2)$, a Eq. (20) ajuda a concluir que

$$I(X;Y) = 1 - \int_{-\infty}^{\infty} p(y|1) \log_2 \left(1 + e^{-2\mu y/\sigma^2} \right) dy \tag{24}$$

8.3.1.1 Caso particular de Y ser uma v.a. gaussiana consistente

Se a variável Y for gaussiana e consistente, $\mathcal{N}(\pm\frac{\sigma^2}{2}, \sigma^2)$, a Eq. (24) simplifica-se em

$$I(X;Y) = 1 - \int_{-\infty}^{\infty} p(y|1) \log_2 \left(1 + e^{-y} \right) dy \tag{25}$$

em que, naturalmente,

$$p(y \mid 1) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left[-\frac{(y - \sigma^2/2)^2}{2\sigma^2} \right]$$

8.3.1.2 *Os casos particulares da informação extrínseca L_e e da informação a priori L_a*

Se nas equações anteriores substituirmos Y por L_a ou L_e obtemos expressões para $I_A = I(X;L_a)$ ou $I_E = I(X;L_e)$, respectivamente. Assim, para I_E teremos

$$I_E = I(X;L_e) = \frac{1}{2}\sum_{x\in\{\pm 1\}}\int_{-\infty}^{\infty} p(L_e|x)\log_2\frac{2\,p(L_e|x)}{p(L_e|-1)+p(L_e|1)}dL_e \tag{26}$$

em vez da Eq. (22), qualquer que seja a fdp de L_e, e

$$I(X;L_e) = 1-\int_{-\infty}^{\infty} p(L_e|1)\log_2\left(1+e^{-L_e}\right)dL_e \tag{27}$$

em vez da Eq. (25), se L_e for modelizada como uma v.a. gaussiana consistente [11] [12]. A informação mútua média I_A é expressa de modo idêntico. Na prática estas expressões têm de ser calculadas por integração numérica, normalmente pelas fórmulas do trapézio ou de Simpson.

Aparte: Recordam-se aqui as fórmulas de integração numérica do trapézio e de Simpson. Suponhamos que queremos determinar $\int_a^b f(x)dx$ e que y_0, y_1, y_2, … são valores igualmente espaçados de $y = f(x)$ no intervalo $[a, b]$.

Fórmula do trapézio: $\int_a^b f(x)dx \approx \frac{b-a}{n}\left(\frac{y_0+y_n}{2}+y_1+y_2+\ldots+y_{n-1}\right)$

n – nº de intervalos em $[a, b]$

Fórmula de Simpson: $\int_a^b f(x)dx \approx \frac{b-a}{6m}\left[\left(y_0+y_{2m}+2(y_2+y_4+\ldots+y_{2m-2})+4(y_1+y_3+\ldots+y_{2m-1})\right)\right]$

$n = 2m$ – nº (par) de intervalos em $[a, b]$

8.3.2 *Caso particular: símbolos X binários com probabilidades quaisquer*

Se os bits $x = \pm 1$ tiverem probabilidades $p(1)$ e $p(-1) = 1 - p(1)$ a Eq. (23) generaliza-se [14] em

$$I(X;Y) = H\left[p(1)\right]-\int_{-\infty}^{\infty} p(y|1)\log_2\left[1+\frac{p(y|-1)}{p(y|1)}\right]dy$$

em que $H[p(1)]$ é a entropia da fonte binária X.

9. Apêndice A4
O limiar de convergência de códigos LDPC regulares em canal BEC

Consideremos um código LDPC (d_v,d_c) cujo limiar de convergência em canal BEC, q_{lim}, desejamos determinar. Seguindo [19] precisamos, primeiro, de encontrar o valor da abcissa do "EXIT chart" para o qual as funções aí representadas,

$$I_{E_v} = 1-q\left(1-I_{A_v}\right)^{d_v-1} \qquad \text{e} \qquad I_{A_c} = I_{E_c}^{\,1/(d_c-1)},$$

são tangentes. Para isso deveremos igualar não só as duas funções (para determinar o seu ponto de intersecção) mas também as suas derivadas (para garantir que os declives nesse ponto são iguais). Como ambas as funções partilham o mesmo eixo das abcissas vamos substituir as variáveis I_{Av} e I_{Ec} pela variável única I. Igualando as funções e derivando membro a membro obtemos o sistema de duas equações

$$\begin{cases} 1-q\left(1-I\right)^{d_v-1} = I^{1/(d_c-1)} \\ q(d_v-1)\left(1-I\right)^{d_v-2} = \dfrac{1}{d_c-1} I^{(2-d_c)/(d_c-1)} \end{cases}$$

Se eliminarmos q obtemos a nova equação

$$\left[\left(d_c-1\right)\left(d_v-1\right)-1\right] I^{\frac{1}{d_c-1}} + I^{\frac{2-d_c}{d_c-1}} - \left(d_c-1\right)\left(d_v-1\right) = 0 .$$

A sua raiz é o ponto de tangência que procuramos. Como a equação ainda está complicada, simplifiquemo-la: 1) fazendo a substituição de variável $x = I^{1/(d_c-1)}$, $0 \le x \le 1$, para obtermos expoentes inteiros,

$$\left[\left(d_c-1\right)\left(d_v-1\right)-1\right] x + x^{2-d_c} - \left(d_c-1\right)\left(d_v-1\right) = 0 ,$$

2) multiplicando ambos os membros por x^{d_c-2} para obtermos expoentes positivos,

$$\left[\left(d_c-1\right)\left(d_v-1\right)-1\right] x^{d_c-1} - \left(d_c-1\right)\left(d_v-1\right) x^{d_c-2} + 1 = 0 .$$

Após encontrarmos uma solução desta equação no intervalo]0; 1[(seja $x_{\lim}$) a abcissa de tangência é calculada de acordo com $I_{\lim} = x_{\lim}^{d_c-1}$ e depois é fácil determinar o limiar $q_{\lim}$:

$$q_{\lim} = \frac{I_{\lim}^{\frac{2-d_c}{d_c-1}}}{\left(d_c-1\right)\left(d_v-1\right)\left(1-I_{\lim}\right)^{d_v-2}}$$

10. Apêndice A5
Relação entre percentagens de nós e de ramos em códigos LDPC irregulares

Suponhamos que num grupo de nós (de variáveis ou de paridade) do grafo de Tanner de um código LDPC irregular o maior grau é D e que b_i representa genericamente a percentagem de ramos ligados a nós de grau i (b_i é λ_i ou ρ_i consoante o tipo de nó). A percentagem b_i está relacionada com a percentagem a_i de nós através de

$$b_i = \frac{a_i i}{\bar{d}} ,$$

em que $\bar{d} = \sum_{i=1}^{D} a_i i$ é o grau médio dos diferentes graus e $\sum_{i=1}^{D} a_i = 1$. Inversamente, a percentagem de nós a_i relaciona-se com b_i através de

$$a_i = \frac{N}{n'} \frac{b_i}{i} ,$$

onde N representa o número total de ramos do grafo de Tanner, isto é, o número de "uns" da matriz **H**, e n' é igual a n ou a $n-k$ consoante se trate de nós de variáveis ou de paridade, respectivamente. Os graus médios dos nós de variáveis e de paridade, $\bar{d}_v$ e $\bar{d}_c$, estão relacionados com o número total de ramos através de $N = n\bar{d}_v = (n-k)\bar{d}_c$ (compare-se com a Eq. (11) dos códigos LDPC regulares). Daqui se tira que

$$\bar{d}_v = (1-R_c)\bar{d}_c . \qquad (28)$$

Se todos os nós de paridade tiverem o mesmo grau d_c então $\bar{d}_v = (1-R_c)d_c$ e $\lambda_i = \frac{a_i i}{(1-R_c)d_c}$. Se todos os nós de variáveis tiverem o mesmo grau d_v então $\rho_j = \frac{a_j j}{d_v}(1-R_c)$.

Manipulando equações e substituindo variáveis conseguimos obter expressões que dependem apenas das fracções λ_i e ρ_j:

$$a_i = \frac{b_i/i}{\sum_k b_k/k} \qquad \bar{d}_v = \frac{1}{\sum_k \lambda_k/k} \qquad \bar{d}_c = \frac{1}{\sum_k \rho_k/k} \qquad R_c = 1 - \frac{\sum_k \rho_k/k}{\sum_k \lambda_k/k}$$

Tomemos como exemplo o código irregular com polinómios $\lambda(x) = \frac{7}{12}x + \frac{1}{4}x^2 + \frac{1}{6}x^3$ e $\rho(x) = \frac{1}{6}x^3 + \frac{5}{6}x^4$ da Fig. 14, onde $\sum_{k=2}^{4} \lambda_k/k = 5/12$ e $\sum_{k=4}^{5} \rho_k/k = 5/24$. Com facilidade confirmamos analiticamente que, por exemplo, 70% dos nós de variáveis têm grau 2 ($\frac{7/(12\times 2)}{5/12} = 0,7$) e 20% dos nós de paridade têm grau 4 ($\frac{1/(6\times 4)}{5/24} = 0,2$). Os graus médios dos nós de variáveis e de paridade são, respectivamente, $\bar{d}_v = \frac{1}{5/12} = 2,4$ e $\bar{d}_c = \frac{1}{5/24} = 4,8$ e a taxa do código é, como se previa, $R_c = 1 - 2,4/4,8 = 0,5$.

11. Referências

[1] S. ten Brink, "Convergence behavior of iteratively decoded parallel concatenated codes", *IEEE Trans. on Communications*, vol. 49, pp. 1727-1737, Outubro de 1999.

[2] C. Berrou, A. Glavieux e P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding," *Proc. of the International Conference on Communications* (ICC '93), Maio de 1993, pp. 1064-1070.

[3] S. A. Abrantes, "Do algoritmo BCJR à descodificação turbo", FEUP, Abril 2004. Acessível *online* em http://paginas.fe.up.pt/~sam/textos/De%20BCJR%20a%20turbo.pdf (24-1-06).

[4] S. A. Abrantes, "Descodificação iterativa de códigos LDPC por transferência de mensagens em grafos de factores", FEUP, Julho 2005. Acessível *online* em http://paginas.fe.up.pt/~sam/textos/LDPC_Tanner.pdf (3-3-06).

[5] M. Tüchler, S. ten Brink e J. Hagenauer, "Measures for Tracing Convergence of Iterative Decoding Algorithms", *Proc. 4th Intern. ITG Conf. on Source and Channel Coding*, Berlim, pp. 53-60, Jan. 2002.

[6] T. J. Richardson e R. L. Urbanke, "The capacity of low-density parity check codes under message-passing decoding", *IEEE Trans. Inform. Theory*, vol. 47, nº 2, pp. 599–618, Fev. 2001.

[7] T. J. Richardson, M. Shokrollahi e R. L. Urbanke, "Design of Capacity-Approaching Irregular Low-Density Parity-Check Codes", *IEEE Trans. Inform. Theory*, vol. 47, nº 2, pp. 619–637, Fev. 2001.

[8] S.-Y. Chung, T. J. Richardson e R. L. Urbanke, "Analysis of Sum-Product Decoding of Low-Density Parity-Check Codes Using a Gaussian Approximation", *IEEE Trans. Inform. Theory*, vol. 47, nº 2, pp. 657-670, Fev. 2001.

[9] A. Roumy, A. J. Grant, I. Fijalkow, P. D. Alexander e D. Pirez, "Turbo-Equalization: Convergence Analysis", *Proc. ICASSP*, nº 4, pp. 2645-2648, 2001.

[10] P. D. Alexander, A. J. Grant e M. C. Reed, “Iterative Detection in Code-Division Multiple-Access with Error Control Coding”, *European Transactions on Telecommunications*, Vol. 9, nº 5, pp. 419-425, Setembro-Outubro de 1998.

[11] N. Wiberg, “Codes and Decoding on General Graphs”, Tese de Doutoramento, Departamento Engenharia Electrotécnica, Univ. Linkoping, Suécia, 1996.

[12] D. Divsalar, S. Dolinar e F. Pollara, “Iterative Turbo Decoder Analysis Based on Density Evolution”, Jet Propulsion Laboratory, California Institute of Technology, TMO Progress Report 42-144, pp. 1-33, 15-2-2001.

[13] I. Land, P. A. Hoeher e S. Gligorevic, "Computation of Symbol-Wise Mutual Information in Transmission Systems with Log-APP Decoders and Application to EXIT Charts", *Proc. Int. ITG Conf. on Source and Channel Coding*, Erlangen, Alemanha, pp. 195-202, 2004.

[14] J. Hagenauer, “The EXIT Chart – Introduction to Extrinsic Information Transfer in Iterative Processing”, *12th European Signal Processing Conference (EUSIPCO 2004)*, Viena, Áustria, 6-9-2004.

[15] A. Ashikhmin, G. Kramer e S. ten Brink, “Extrinsic Information Transfer Functions: Model and Erasure Channel Properties”, *IEEE Trans. Inform. Theory*, vol. 50, nº 11, pp. 2657-2673, Nov. 2004.

[16] S. ten Brink, G. Kramer e A. Ashikhmin, “Design of Low-Density Parity-Check Codes for Modulation and Detection”, *IEEE Trans. Communications*, vol. 52, nº 4, pp. 670-678, Abril 2004.

[17] C. Schlegel e L. Perez, *Trellis and Turbo Coding*, Wiley-IEEE Press, 2003.

[18] T. J. Richardson, A. Shokrollahi e R. L. Urbanke, "Design of provably good low-density parity-check codes”, *IEEE Trans. Inform. Theory*, vol. 47, nº 2, pp. 619-637, Fev. 2001.

[19] T. Hehn, A. Dönmez e J. B. Huber, “Exact Thresholds for LDPC Codes Transmitted Over Binary Erasure Channels”, *Proceedings of 43rd Annual Allerton Conf. on Communication, Control, and Computing*, Monticello, USA, Set. 2005.